Autoreferat

Karol Horodecki

17 kwietnia 2019

1. Imiona i nazwisko

   Karol Mieczysław Horodecki

2. Posiadane dyplomy i stopnie naukowe

   - dyplom magistra matematyki ze spec. informatyka i metody numeryczne, Uniwersytet Gdański, Wydział Matematyki Fizyki i Informatyki 2004
   - stopień doktora nauk matematycznych w zakresie informatyka, Uniwersytet Warszawski, Wydział Matematyki, Informatyki i Mechaniki 2009

3. Dotychczasowe zatrudnienie w jednostkach naukowych:

   - stanowisko asystenta w Instytucie Informatyki Uniwersytetu Gdańskiego (10.02.2008 - 30.04.2009)
   - stanowisko adiunkta w Instytucie Informatyki Uniwersytetu Gdańskiego od 1.05.2009

4. Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. 2017 r. poz. 1789):

   (a) Tytuł osiągnięcia naukowego:

   "Wybrane, wzajemne relacje między nielokalnością Bella, kontekstualnością, kluczem kryptograficznym bezpiecznym względem kwantowego adwersarza i kwantowym splątaniem."

KH

(b) Lista publikacji wchodzących w skład w.w. osiągnięcia

[H1] Karol Horodecki. „On Distinguishing of Non-Signaling Boxes via Completely Locality Preserving Operations". *IEEE Trans. Inf. Theory* 63.9 (wrz. 2017), 5666–5683.

[H2] Karol Horodecki, Andrzej Grudka, Pankaj Joshi, Waldemar Kłobus i Justyna Łodyga. „Axiomatic approach to contextuality and nonlocality". *Physical Review A* 92 (wrz. 2015), s. 032104. arXiv: 1506.00509. wraz z erratą *Physical Review A* 99, 039901(E) (mar. 2019).

[H3] Karol Horodecki i Gláucia Murta. „Bounds on quantum nonlocality via partial transposition". *Physical Review A(R)* 92 (lip. 2015), s. 010301. arXiv: 1407.6999.

[H4] Stefan Bäuml, Matthias Christandl, Karol Horodecki i Andreas Winter. „Limitations on quantum key repeaters". *Nature Communications* 6 (kw. 2015), s. 6908. arXiv: 1402.5927.

[H5] Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Ryszard Horodecki, Pankaj Joshi, Waldemar Kłobus i Antoni Wójcik. „Quantifying Contextuality". *Physical Review Letters* 112.12 (mar. 2014). arXiv: 1209.3745.

[H6] P. Joshi, Michał Horodecki, Ryszard Horodecki, Andrzej Grudka, Karol Horodecki i Paweł Horodecki. „No-broadcasting of non-signalling boxes via operations which transform local boxes into local ones". *Quantum Inf. Comp.* 13.7-8 (lip. 2013), s. 567–582. arXiv: 1111.1781.

[H7] Konrad Banaszek, Karol Horodecki i Paweł Horodecki. „Quantum privacy witness". *Physical Review A* 85 (sty. 2012), s. 012330. arXiv: 1109.2486.

(c) Omówienie celu naukowego ww. prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania.

Ten podpunkt autoreferatu jest opisany następująco. W sekcji 1 przedstawiam tło problemu podjętego w cyklu prac oraz cel tego cyklu. Sekcja 2 wprowadza pojęcia niezbędne do opisu rezultatów. W jej kolejnych podsekcjach opisuję pojęcia kwantowego splątania 2.1, kwantowego klucza kryptograficznego bezpiecznego względem kwantowego adwersarza 2.2, nielokalności Bella 2.3 i kontekstualności 2.4, wraz z notacją wykorzystywaną w następnych sekcjach. W sekcji 3, w kolejnych podpunktach 1)-7) opisuję wyniki prac [H1-H7].

Odnośniki literaturowe zaczynające się od litery H np. [H1], odnoszą się do publikacji, które stanowią część osiągnięcia. Odwołania zaczynające się na literę P i D (np. [P1] i [D1]) odnoszą się do publikacji aplikującego z listy filadelfijskiej, które powstały odpowiednio po oraz przed doktoratem. Pozostałe publikacje, których jestem współautorem są oznaczane literą I (np. [I1]). Literatura przedmiotu jest oznaczana listą pierwszych liter nazwisk autorów i rokiem publikacji, np. [BB84] lub skrótem pierwszego nazwiska w przypadku większej liczby autorów np. [Ben+93].

1 Wprowadzenie

Kwantowa teoria informacji powstała z połączenia kryptografii z mechaniką kwantową [Wie83, BB84] dzięki zjawisku kwantowego zakazu klonowania [WZ82, Die82]. Jednakże pierwszym kwantowym zjawiskiem, które zostało rozpoznane jako zasób, było tzw. *kwantowe splątanie* [Ben+96a, Ben+96b]. Stało
się tak między innymi dlatego, że, jak odkryto, czysty kwantowy stan splątany może zostać wykorzystany między innymi do kwantowej teleportacji [Ben+93] oraz kwantowego gęstego kodowania [BW92]. Zjawisko kwantowego splątania zostało również zbadane jako zasób w terminach tego, co dziś nazywamy teorią zasobu [Ben+96b, D1]. Wedle tego podejścia, teorię zasobu określają trzy obiekty:

1) Zbiór stanów S.
2) Zbiór stanów darmowych $F_s \subseteq S$.
3) Zbiór operacji darmowych F_o, które można wykonać na stanach z S.

Z teorią zasobu związanych jest również kilka ważnych pojęć, takich jak:

- *miara zasobu* - jest to funkcja, która nie wzrasta ze względu na operacje darmowe F_o: Miara zasobu może być *operacyjna*: np. maksymalna ilość zasobu, który można otrzymać z danego stanu $s \in S$ za pomocą operacji ze zbioru F_o. Może też nie mieć takiej interpretacji czyli być *abstrakcyjna*. Zwykle miary abstrakcyjne są tworzone po to, aby stanowić ograniczenia dolne lub górne

na miary operacyjne; dobre z fizycznego punktu widzenia miary zasobu mają cechę nazywaną *asymptotyczną ciągłością*, tj. różnią się na stanach bliskich sobie o ϵ niewiele, konkretnie o funkcję postaci $C\epsilon \log_2 d + f(\epsilon)$, gdzie d jest wymiarem stowarzyszonym ze stanem, zaś f funkcją, która zbiega do zera wraz z malejącym ϵ i nie zależy od wymiaru d a C jest stałą niezależną od d.

- *zbiór stanów zawierających zasób w idealnej postaci* (tj. bez domieszki szumu).
- *świadek zasobu* - jest to wielkość obserwowalna (w przypadku Mechaniki Kwantowej - "obserwabla"), której wartość średnia na każdym stanie darmowym jest $\geqslant 0$, zaś na pewnym stanie nienależącym
  do F_s, jest < 0. Pomiar świadka zasobu jest ekonomicznym sposobem pomiaru ilości tego zasobu.

Jednym z istotnych zagadnień w teorii zasobu jest znalezienie odpowiedzi na następujące pytanie:

- Jakie przekształcenia stanów zawierających zasób można wykonać za pomocą darmowych operacji ?

Przykładowym problemem z tej klasy jest znalezienie odpowiedzi na pytanie: *Mając dane n kopii stanu wejściowego ρ_{we} ile kopii m stanu ρ_{wy}, który jest bliski do stanu zawierającego zasób w idealnej postaci możemy otrzymać?*. Stosunek m/n do w granicy wielu kopii n jest nazywany miarą *destylowalnego* zasobu, a proces otrzymywania zasobu w postaci bliskiej do idealnej za pomocą operacji darmowych jest nazywany *destylacją zasobu*.

W ostatnich latach zidentyfikowano i częściowo zbadano co najmniej kilkanaście zasobów, zarówno kwantowych, jak i poza-kwantowych (zob. [CG18]). Jedne z nich można otrzymać fizycznie za pomocą stanów i operacji spełniających założenia Mechaniki Kwantowej. Inne można otrzymać jedynie w ramach teorii, które są bardziej ogólne niż Mechanika Kwantowa i współdzielą z nią jedynie niektóre cechy: na przykład niemożność przesyłania informacji szybciej niż z prędkością światła. Ma to miejsce w przypadku teorii w której stanami są rozkłady wrunkowe, będącej szczególnym przypadkiem Teorii Uogólnionego Prawdopodobieństwa [Bar05, PR92].

Teorie zasobów różnią się najczęściej zbiorem operacji darmowych F_o, ale także niekiedy przestrzenią stanów S. Z tego też względu, jedne fakty zachodzą w pewnych teoriach, a w innych nie. Ważnym dla dalszych rozważań przykładem jest fakt, że w teorii splątania można za pomocą darmowych operacji wykonać przekazanie splątania (ang. "entanglement swapping") [Żuk+93], zaś w ogólnej teorii probabilistycznej *niesygnalizujących rozkładów warunkowych*, innymi słowy w teorii zasobu jakim jest nielokalność [Bel64, Tsi87, PR92], nie zachodzi analogiczna możliwość przekazywania nielokalności [SPG06]. Niemniej, w przypadku kwantowej teorii niesygnalizujących rozkładów warunkowych (gdy zawężamy się tylko do tych rozkładów, które można otrzymać przez pomiar ze stanu kwantowego) splątanie i nielokalność są istotnie powiązane: warunkiem koniecznym (choć nie wystarczającym [Wer89]), aby rozkład warunkowy zawierał zasób nielokalności jest to, aby był splątany, czyli zawierał zasób splątania. Z tego względu zasadne jest badanie wzajemnych relacji między różnymi zasobami, przez wykazywanie analogii bądź jej braku.

Celem jednotematycznego zbioru prac [H1, H2, H3, H4, H5, H6, H7], jest ukazanie wzajemnych relacji między zasobami *nielokalności Bella* [H1, H6, H3], *kontekstualności* [H2, H5], *klucza kryptograficznego* (bezpiecznego względem kwantowego adwersarza)[1] [H7, H4] oraz kwantowego splątania [D1], przez wykazanie zachodzących w przypadku jednego z pierwszych trzech zasobów analogicznych faktów do tych mających miejsce w przypadku innego (lub więcej niż jednego) z wymienionych czterech zasobów. Poniżej w sekcji 2 wprowadzam najpierw opisane wyżej pojęcia dla czterech wymienionych tu zasobów, a następnie w sekcji 3 opisuję rezultaty osiągnięcia.

2 Kwantowe splątanie, klucz kryptograficzny, nielokalność Bella i kontekstualność

Poniżej krótko wprowadzam cztery zasoby: kwantowe splątanie, kwantowe bezpieczeństwo (tj. bezpieczeństwo klucza kryptograficznego względem kwantowego adwersarza), jak również nielokalność Bella oraz kwantową kontekstualność, wraz z notacją potrzebną do ich opisu.

[1] W dalszej części tekstu, o ile nie jest powiedziane inaczej, przez klucz kryptograficzny rozumiemy klucz kryptograficzny bezpieczny względem kwantowego adwersarza.

2.1 Kwantowe splątanie jako zasób

W przypadku kwantowego splątania zbiór S to zbiór $n \geqslant 2$-układowych macierzy gęstości ρ, tj. macierzy o współczynnikach zespolonych, spełniających warunek $Tr\rho = 1$, $\rho \geqslant 0$. Zbiór F_s to zbiór stanów *separowalnych*, czyli stanów będących mieszanką probabilistyczną stanów produktowych $F_s = \{\rho \in S : \rho = \sum_{i_1,\ldots,i_n} p_{i_1,\ldots,i_n} \rho_{i_1} \otimes \ldots \otimes \rho_{i_n}, \sum_{i_1,\ldots,i_n} p_{i_1,\ldots,i_n} = 1, p_{i_1,\ldots,i_n} \geqslant 0\} \equiv SEP(A_1 : \ldots : A_n)$. W przypadku dwóch podukładów, używamy notacji $SEP(A : B)$. Wszystkie stany niedarmowe (tj. nie będące separowalnymi) są nazywane stanami *splątanymi*.

Natomiast naturalny zbiór darmowych operacji F_o, to w przypadku teorii splątania zbiór lokalnych operacji kwantowych i klasycznej komunikacji (LOKK). Bez wdawania się w nieistotne dla dalszych rozważań szczegóły definicji, możemy powiedzieć, że operacja LOKK jest złożeniem (niekoniecznie skończonej liczby) operacji kwantowych na odpowiednich podukładach oraz komunikacji z jednego podukładu do drugiego etykiet wyników tychże operacji tak by kolejna operacja na podukładzie (operacje na podukładach są wykonywane naprzemiennie) mogła być warunkowana wynikiem poprzedniej. Analogicznie możemy mówić o większej liczbie podukładów (np. trzy: A, B, C) i o różnych wariantach komunikacji (np. $A \rightarrow B \leftrightarrow C$, gdy A może komunikować wyniki pomiarów tylko do C, zaś C i B mają komunikację obustronną).

Przykładową *miarą kwantowego splątania* jest *splątanie destylowalne* E_D [Ben+96a], zdefiniowane jak następuje:

$$E_D(\rho) := \inf_{\epsilon>0} \limsup_{n\to\infty} \sup_{\Lambda_n \in LOKK} \{\frac{m}{n} : \Lambda_n(\rho^{\otimes n}) \approx_\epsilon |\Psi\rangle\langle\Psi|^{\otimes m}\} \tag{1}$$

gdzie $\rho \approx_\epsilon \sigma$ oznacza odległość w normie śladowej $||\rho - \sigma||_{tr} = \frac{1}{2}Tr|\rho - \sigma|$, pomiędzy dwoma stanami kwantowymi ρ, σ, zaś $|\Psi\rangle$ jest stanem reprezentującym idealny zasób - stanem maksymalnie splątanym, określonym
z dokładnością do obrotów unitarnych na podukładach jako

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2^m}} \sum_{i=0}^{2^m-1} |ii\rangle. \tag{2}$$

Dualną miarą do destylowalnego splątania jest tzw. *koszt splątania* [Ben+96a], który zdefiniowany jest następująco:

$$E_C(\rho) := \inf_{\epsilon>0} \limsup_{n\to\infty} \sup_{\Lambda_n \in LOKK} \{\frac{m}{n} : \Lambda_n(|\Psi\rangle\langle\Psi|^{\otimes m}) \approx_\epsilon \rho^{\otimes n}\}. \tag{3}$$

Miarą, która ogranicza z góry destylowalne splątanie jest *względna entropia splątania* [Ved+97], zdefiniowana tak:

$$E_R(\rho_{AB}) := \inf_{\sigma \in SEP(A:B)} D(\rho||\sigma), \tag{4}$$

gdzie $D(\rho||\sigma) := Tr\,\rho\log\rho - Tr\,\rho\log\sigma$ dla dwóch macierzy gęstości ρ, σ[2].

Powyższa miara kwantowego splątania jest *asymptotycznie ciągła*. Konkretnie spełnia ona warunek:

$$|E_R(\rho) - E_R(\rho')| \leqslant \epsilon \log d + (1+\epsilon)h(\frac{\epsilon}{1+\epsilon}) \tag{5}$$

jeśli tylko $\rho \approx_\epsilon \rho'$, które są macierzami $d \times d$, zaś h jest binarną entropią Shannona, zdefiniowaną jako $h(z) = -z\log_2 z - (1-z)\log_2(1-z)$ [DH99]. Inną istotną dla naszych rozważań miarą jest miara nazwana zmniejszonym splątaniem (ang. "*squashed entanglement*") [CW04, Tuc02], która jest zdefiniowana następująco:

$$I_{sq}(\rho_{AB}) = \inf_{\Lambda_E} I(A : B|E)_{I_{AB}\otimes\Lambda_E|\psi_{ABE}\rangle}, \tag{6}$$

gdzie warunkowa wzajemna informacja ma postać $I(A : B|E) = S(AE) + S(BE) - S(E) - S(ABE)$, $S(.)$ jest entropią von-Neumanna stanu kwantowego, a $|\psi_{ABE}\rangle$ jest dowolnym dopełnieniem stanu ρ_{AB} do stanu czystego układów ABE.

Poniżej przypomnę kilka własności kwantowych stanów splątanych oraz przekształceń, których można (bądź nie) na nich wykonać. Będą one istotne dla dalszych rozważań, gdyż zadamy pytanie, czy analogiczne fakty mają miejsce w przypadku innych zasobów:

[2]Zgodnie z konwencją $D(\rho||\sigma) = \infty$ jeśli $\mathrm{supp}(\rho) \cap \mathrm{supp}(\sigma) \neq \emptyset$.

KR

- splątanie kwantowe w postaci stanu czystego maksymalnie splątanego jest przekazywalne (ang. swappable), tj. istnieje operacja kwantowa $\Lambda \in LOKK(A : C_1C_2 : B)$, taka że

$$\Lambda(|\Psi\rangle_{AC_1} \otimes |\Psi\rangle_{C_2B}) = |\Psi\rangle_{AB}, \tag{7}$$

  gdzie $|\Psi\rangle$ jest stanem czystym, maksymalnie splątanym [Żuk+93, Ben+93].

- za pomocą operacji LOKK nie można odróżnić w pełni bazy stanów maksymalnie splątanych, które tworzą bazę [Gho+01, D2]. Pewnych stanów, prawie ortogonalnych, nie można odróżnić od siebie za pomocą operacji PPT, tj. operacji pozostających kompletnie dodatnimi i zachowującymi ślad, po wykonaniu częściowej transpozycji na operatorach Krausa tworzących operację[Ben+99, Egg+01].

Jako, że kwantowe splątane jest zasobem, kolejna jego własność wyraża się następująco:

- kwantowe splątanie jest nierozgłaszalne za pomocą operacji LOKK, tj. przekształcenie $\Lambda(\rho_{AB}) = \tau_{ABA'B'}$ takie że odpowiednie podukłady stanu τ, są równe ρ_{AB}: $\tau_{AB} = \tau_{A'B'} = \rho_{AB}$ nie jest możliwe jeśli $\Lambda \in LOKK$, zaś stan ρ_{AB} jest splątany [H6].

2.2 Klucz kryptograficzny bezpieczny względem kwantowego adwersarza

Przedstawię teraz pojęcie klucza [BB84] bezpiecznego względem kwantowego adwersarza w ujęciu teorii zasobów. Zgodnie z opisem [D3, D4], zbiorem stanów w tej teorii, S_{key} jest, podobnie jak w przypadku teorii splątania, zbiór wszystkich stanów kwantowych: $S_{key} = S_{ent}$. Zbiorem operacji darmowych jest również ten sam zbiór LOKK. Jako zbiór stanów darmowych jest obecnie przyjmowany, podobnie jak w przypadku kwantowego splątania, zbiór stanów separowalnych $F_{key} = SEP$, gdyż problem istnienia stanów, które byłyby splątane, ale nie można było z nich otrzymać klucza kryptograficznego jest, jak dotąd, otwarty. W takim ujęciu teoria splątania i bezpieczeństwa kwantowego różnią się jedynie zbiorem stanów reprezentujących idealny zasób. Zostały one scharakteryzowane jako stany postaci

$$\gamma_{AA'BB'} = \sum_{i,j=0}^{d-1,d-1} \frac{1}{d} |ii\rangle\langle jj|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger \tag{8}$$

gdzie U_i dla $i \in \{0, ..., d-1\}$ są transformacjami unitarnymi, zaś $\sigma_{A'B'}$ jest dowolnym stanem układu $A'B'$ [D3, D4].

Co istotne, stany bezpieczne po pomiarze układu AB w bazie obliczeniowej $\{|ij\rangle\}$, otrzymujemy wyniki pomiarów które są (i) skorelowane ze sobą (ii) losowe oraz (iii) niezależne od podukładu *puryfikacji*[3] $\gamma_{AA'BB'}$ do stanu czystego. Fakt ten wyjaśnia, dlaczego stany te reprezentują klucz kryptograficzny bezpieczny względem kwantowego adwersarza: losowy ciąg bitów nieznany nikomu oprócz osób zaufanych A i B (zwykle zwanych Alicją i Bogdanem) stanowi klucz, może bowiem być wykorzystany do bezpiecznej komunikacji za pomocą protokołu zwanego "one-time-pad". Szyfrowanie w tym protokole polega na wykonaniu bit po bicie (wiadomości zakodowanej binarnie) operacji xor z bitami ciągu reprezentującego wspomniany klucz. Dekodowanie przebiega tak samo: ciąg szyfrogramu jest xor-owany bit po bicie z kluczem. Taki klucz otrzymany ze stanu bezpiecznego przez pomiar gwarantuje bezpieczeństwo względem kwantowego adwersarza, gdyż dopełnienie do stanu czystego (wspomniana *puryfikacja*) jest stanem, którego podukład E daje maksymalną wiedzę, jaką może mieć podsłuchiwacz o układach $ABA'B'$ (ang. eavesdropper stąd nazywany Ewą) zgodnie z opisem Mechaniki Kwantowej.

Odpowiednikiem miary E_D w przypadku zasobu jakim jest *klucz kryptograficzny* jest następująca, zwana *kluczem destylowalnym*:

$$K_D(\rho) = \inf_{\epsilon>0} \limsup_{n\to\infty} \sup_{\Lambda_n \in LOKK} \{\frac{m}{n} : \Lambda_n(\rho^{\otimes n}) \approx_\epsilon \gamma^{(m)}\}, \tag{9}$$

[3]Przez puryfikację stanu (8) do stanu czystego trójukładowego $|\psi_{AA'BB'E}\rangle$ (A i A' są rozważane razem, podobnie jak B i B'), tj. opisanego przez wektor przestrzeni Hilberta, rozumiemy stan dla którego ślad częściowy po podukładzie E spełnia: $Tr_E|\psi\rangle\langle\psi|_{AA'BB'E} = \gamma_{AA'BB'}$.

gdzie $\gamma^{(m)}$ jest stanem bezpiecznym, którego podukład AB (tzw. część klucza) jest wymiaru $d \times d$ przy $d = 2^m$.

Istotny dla dalszych rozważań jest fakt, że stany te mogą być przybliżane przez stany zachowujące dodatniość częściowej transpozycji. Ich zbiór jest oznaczony jako $PPT = \{\rho : I \otimes T\rho \geqslant 0\}$. O stanach tych wiadomo, że nie zawierają destylowalnego splątania [HHH98] tj. $\rho \in PPT \Rightarrow E_D(\rho) = 0$. Znane są również konstrukcje stanów ze zbioru PPT (dalej zwane *stanami PPT*), które zawierają więcej klucza kryptograficznego niż kwantowego splątania [DW05, D3, D5], $0 = E_D < K_D \approx 1$. Wiadomo również, że podobny warunek spełniają niektóre stany bezpieczne, nie są one jednak stanami PPT (tzw. stany NPT).

2.3 Nielokalność Bella

Przedstawimy teraz pokrótce zasób, jakim jest nielokalność Bella (zarówno kwantowa, tj. pochodząca od stanu kwantowego przez pomiar, jak i poza-kwantowa gdzie taki stan i/lub pomiary nie istnieją) [Bel64, Tsi87, Bru+14]. Przestrzenią stanów w przypadku (w ogólności) *poza-kwantowej nielokalności Bella* jest zbiór *niesygnalizujących* rozkładów warunkowych o ustalonym wymiarze wejść (X, Y) o wartościach $(X = x, Y = y) \in \mathcal{X} \times \mathcal{Y}$ i wyjść $(A = a, B = b) \in \mathcal{A} \times \mathcal{B}$. Niesygnalizujący rozkład warunkowy, to rozkład $P(A, B|X, Y)$ spełniający warunki:

$$\forall_{x,y \in \mathcal{X} \times \mathcal{Y}} P(a, b|x, y) \geqslant 0, \tag{10}$$

$$\sum_{a \in \mathcal{A}, b \in \mathcal{B}} P(a, b|x, y) = 1, \tag{11}$$

$$\forall_{a \in \mathcal{A}, x \in \mathcal{X}, y, y' \in \mathcal{Y}} \sum_b P(a, b|x, y) = \sum_b P(a, b|x, y'), \tag{12}$$

$$\forall_{b \in \mathcal{B}, x, x' \in \mathcal{X}, y \in \mathcal{Y}} \sum_a P(a, b|x, y) = \sum_b P(a, b|x', y). \tag{13}$$

Ostatnie dwa warunki to brak sygnalizowania (przekazywania informacji szybciej niż światło) od podukładu B do A (od Bogdana do Alicji) oraz analogicznie: od Alicji do Bogdana. Zbiór niesygnalizujących rozkładów warunkowych tworzy wielościan. Oznaczamy go tak: $NS(|\mathcal{A}|, |\mathcal{B}|, |\mathcal{X}|, |\mathcal{Y}|)$ lub skrótowo NS, w zależności od kontekstu.

Zbiór operacji darmowych tworzą tzw. operacje obwodowe (ang. "wirings"), czyli dowolne funkcje wejść i wyjść, gdzie w przypadku wielu wejść i wielu wyjść, wyjście jednego rozkładu można zrównać z wejściem drugiego. Najprostsza operacja możliwa do wykonania na rozkładzie warunkowym to "przyciśnięcie przycisków" - tj. ustalenie wartości jego wejść X i Y jako konkretne $x \in \mathcal{X}$ oraz $y \in \mathcal{Y}$ [Bru+14].

Zbiorem rozkładów darmowych jest zbiór $L(|\mathcal{A}|, |\mathcal{B}|, |\mathcal{X}|, |\mathcal{Y}|)$ (lub skrótowo L), tzw. rozkładów *lokalno-realistycznych* postaci: $P_L(A, B|X, Y) := \sum_i \lambda_i P(A|X, \lambda_i) P(B|Y, \lambda_i)$, gdzie $\sum_i \lambda_i = 1 \lambda_i \geqslant 0$. Są to rozkłady, które mają z góry predefiniowane wyniki pomiarów (dla każdego z podukładów), przed wykonaniem tych pomiarów.

Jedną z miar nielokalności, jest tzw. *frakcja nielokalności* (lub *koszt nielokalności*) [Bru+11], zdefiniowana następująco:

$$C(P) = \inf\{p | pN + (1 - p)P_L = P,\ N \in NS,\ P_L \in L\}. \tag{14}$$

Świadek nielokalności, to tzw. *nierówność Bella* [Bel64], czyli zestaw liczb $S := \{s_{a,b}^{x,y}\}$, który spełnia warunek, dla pewnej stałej C_L:

$$\forall_{P_L \in L} \sum_{a,b,x,y} s_{a,b}^{x,y} P_L(a, b|x, y) \leqslant C_L, \tag{15}$$

$$\exists_{P \in NS} \sum_{a,b,x,y} s_{a,b}^{x,y} P(a, b|x, y) > C_L, \tag{16}$$

(powyżej założyliśmy, że $C_L \geqslant 0$; nierówności są przeciwne, w przypadku gdy $C_L < 0$). Gdy $s_{a,b}^{x,y} \in \{0, 1\}$, nierówność Bella nazywana jest grą. W ogólności jej współczynniki nie muszą być jednak liczbami rzeczywistymi.

KM

Mówimy o *kwantowej nielokalności Bella*, gdy ograniczamy się do podzbioru $Q \subset NS$ rozkładów warunkowych, oznaczonych jako $Q(|\mathcal{A}|, |\mathcal{B}|, |\mathcal{X}|, |\mathcal{Y}|)$, spełniających: $P(A = a, B = b|X = x, Y = y) = TrM_a^x \otimes M_b^y \rho_{AB}$ dla wszystkich a, b, x, y oraz dla pewnych macierzy spełniających $\sum_a M_a^x = \mathrm{I}$ oraz $\sum_b M_b^y = \mathrm{I}$, $M_a^x, M_b^y \geqslant 0$, czyli będących POVMami. W tym przypadku zbiór rozkładów darmowych to również L, a przestrzeń stanów to Q. Zauważmy, że $L \subset Q \subset NS$.

Na potrzeby poniższych rozważań skupimy się teraz na przypadku wielościanu $NS(2, 2, 2, 2)$. Najbardziej znanym świadkiem nielokalności jest nierówność Bella zwana CHSH [Cla+69] (od pierwszych liter nazwisk odkrywców: Clauser, Horne, Shimony i Holt), która ma postać:

$$CHSH(P) := \frac{1}{4} \sum_{a,b,x,y=0}^{1} \delta(a \oplus b = x.y) P(a, b|x, y) \leqslant \frac{3}{4}, \tag{17}$$

gdzie $\oplus$ jest operacją logiczną XOR (dodawane modulo 2), zaś $\cdot$ jest operacją logiczną AND. Rozkładem warunkowym o maksymalnej ilości zasobu, co zauważyli Popescu i Rohrlich, jest tzw. rozkład warunkowy Popescu-Rohrlich (PR) [PR92]. Łamie on maksymalnie nierówność CHSH. W ogólności jest 8 rozkładów warunkowych z maksymalną nielokalnością w przypadku $NS(2, 2, 2, 2)$, i są one postaci [Bar+05]:

$$B_{rst}(a, b|x, y) := \begin{cases} \frac{1}{2} \text{ if } a \oplus b = x.y \oplus r.x \oplus s.y \oplus t \\ 0 \text{ else.} \end{cases} \tag{18}$$

Spełniają one $CHSH_{rst}(P) = 1$, tj. łamią maksymalnie odpowiednią nierówność typu $CHSH$ - jak w (17), tylko ze zmienionym warunkiem na: $\delta(a \oplus b = x.y \oplus r.x \oplus r.y \oplus t)$, gdzie $r, s, t \in \{0, 1\}$. Fakt ten jest znamienny, gdyż Borys Tsirelson wykazał, że $CHSH(P_Q) \leqslant (2 + \sqrt{2})/4$ dla wszystkich kwantowych rozkładów warunkowych $P_Q \in NS(2, 2, 2, 2)$ [Tsi87], zatem Mechanika Kwantowa nie pozwala na pełną nielokalność w tym przypadku.

2.4 Kontekstualność kwantowa i poza-kwantowa

Zjawisko kwantowej kontekstulaności [KS67] jest cechą zbioru obserwabli $\mathcal{M} = \{M_i\}$ z których część (lecz nie wszystkie) komutują ze sobą tj. spełniają warunek $[M_i, M_j] = 0$, co implikuje, że są współmierzalne. Każdy (maksymalny w sensie teoriomnogościowym) współmierzalny podzbiór $\mathcal{M}$ nazywany jest *kontekstem*. Zbiór wszystkich kontekstów oznaczamy jako $\mathcal{C}$. Przestrzeń stanów tej teorii zasobu[4] to zbiór rozkładów wyników pomiarów każdego kontekstu: $P(a|c)$, który spełnia warunek *konsystencji*: jeśli 2 konteksty mają wspólny podzbiór obserwabli $M_{i_1}, ..., M_{i_k}$, to na tym podzbiorze ich marginalne rozkłady są sobie równe (warunek ten odpowiada warunkowi niesygnalizowania w teorii nielokalności Bella). $|\mathcal{C}|$ kontekstów, etykietowanych przez $c \in \mathcal{C}$ stanowi wymiar "wejścia" rozkładu warunkowego. Dla każdego kontekstu składającego się z obserwabli $\{M_{j_1}, ..., M_{j_n}\}$ wymiar "wyjścia" to $\Pi_{i=1}^{n} a_{j_i}$ gdzie a_{j_i} to liczba wyników obserwabli M_{j_i}. W rozważaniach opisanych poniżej z rozkładem warunkowym $P(a|c)$ stowarzyszamy wymiar postaci $\min\{|\mathcal{C}|, \Pi_{i=1}^{|\mathcal{M}|} a_i\}$.

Zbiorem stanów darmowych jest wielościan rozpięty przez rozkłady deterministyczne $D(a|x)$, które mają wartości wszystkich obserwabli ustalone (w postaci tzw. delt Kroneckera) i spełniają warunek konsystencji (leżą w wielościanie konsystentnych rozkładów warunkowych). Rozkład warunkowy, który jest mieszanką probabilistyczną takich rozkładów nazywany jest rozkładem *niekontekstualnym*. Rozkłady, które nie są niekontekstualne nazywamy *kontekstualnymi*.

Do momentu powstania prac [Ací+15, CFS16, H2] - które powstały niezależnie od siebie, badane były głównie, zgodnie z najlepszą wiedzą autora, przypadki świadków kontekstualności lub kolejne przykłady coraz mniejszych zbiorów obserwabli, wykazujących kontekstualność zależną, bądź niezależną od stanu (zob. [Cab08] i referencje w tej pracy). Kwantowa kontekstualność była była badana jako teoria zasobu w przypadku gdy sprowadza się do nielokalności Bella[5]. W pracy [H2] ujęliśmy tę teorię za pomocą kilku aksjomatów oraz zbadaliśmy obiekty i fakty analogiczne do tych znanych z teorii splątania (patrz podpunkty 5 i 6) sekcji 3).

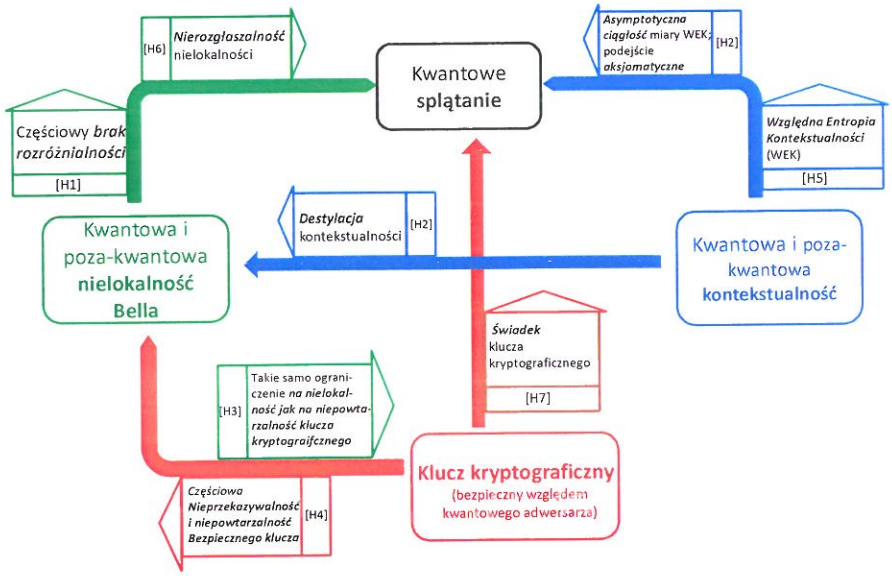
[4] Pytanie czy kontekstualność kwantową należy traktować jako zasób jest kwestią dyskusji. Ostatnie wyniki [How+14, SHP17], wskazują, że odpowiedź na to pytanie jest twierdząca. Niezależnie od odpowiedzi na to pytanie, zjawisko to można badać w ujęciu teorii zasobów.

[5] O nielokalności typu Bella mówimy wtedy, gdy *wszystkie* relacje komutacji w danym zbiorze obserwabli $\mathcal{M}$ wynikają z przestrzennego rozdzielenia obserwabli - rozkłady kontekstualne nazywamy wtedy nielokalnymi.

KH

3 Opis głównych rezultatów osiągnięcia

W tej sekcji przedstawię główne rezultaty publikacji wchodzących w skład osiągnięcia [H1, H2, H3, H4, H5, H6, H7], które ukazują wzajemne powiązania między zasobami nielokalności typu Bella, kontekstualności, klucza kryptograficznego, bezpiecznego względem kwantowego adwersarza - przez analogię do teorii kwantowego splątania, jak również bezpośrednie zależności między nielokalnością Bella i kluczem kryptograficznym oraz kontekstualnością. Jak omówiliśmy w sekcji wstępnej, zasoby te w sposób naturalny są powiązane, gdyż nielokalność typu Bella jest szczególnym przypadkiem kontekstualności, zaś splątanie w postaci stanów czystych, jest szczególnym przypadkiem kwantowego bezpieczeństwa. Poniżej przedstawimy konsekwencje tego faktu, prowadzące do bardziej ścisłych powiązań, dzięki zachodzącym analogiom. Ich syntetyczny obraz jest przedstawiony na Rys. 1.



Rysunek 1: Wizualizacja głównych powiązań zasobów (przez analogię), wykazanych w pracach wchodzących w skład dzieła [H1]-[H7]: kwantowa i poza-kwantowa nielokalność Bella (w analogii do kwantowego splątania) wykazuje takie cechy, jak częściowy brak rozróżnialności rozkładów ekstremalnych w przypadku $NS(2,2,2,2)$[H1] i nierozgłaszalność [H6]. W analogii do kwantowego splątania, można zdefiniować i obliczyć miarę kwantowej i poza-kwantowej kontekstualności, zwanej *względną entropią kontekstualności* (WEK) [H5], zaś w analogii do nielokalności Bella, wykazano, że możliwa jest koncentracja kontekstulaności, a ujęcie obu teorii, może być w analogii do kwantowego splątania aksjomatyczne [H2]. Można zdefiniować i wykazać użyteczność świadka bezpieczeństwa, podobnie jak to ma miejsce w przypadku kwantowego splątania [H7], zaś klucz kryptograficzny w pewnej formie zaszumionej bywa niemożliwy do przekazania w paradygmacie kwantowych powtarzaczy (ang. repeaters), podobnie jak nielokalność Bella, która nie może być przekazywana [H4]. W przypadku stanów o dodatniej częściowej transpozycji względna entropia nielokalności (tj. WEK w przypadku nielokalności) jest ograniczony z góry [H3], tak samo, jak *klucz powtarzalny* [H4].

W ramach niniejszego osiągnięcia zająłem się następującymi zagadnieniami:

1) **Świadek prywatności [H7]**
W analogii do zasobów splątania i nielokalności [D1, Bru+14] zaproponowaliśmy w pracy [H7] dwie konstrukcje świadka klucza kryptograficznego, bezpiecznego względem kwantowego adwersarza. Podaliśmy także ograniczenie dolne na wielkość klucza destylowalnego K_D, dające się wyrazić w terminach skonstruowanych obserwabli. Zagadnienie to jest ważne z punktu widzenia eksperymentu: chcemy wykonać najmniejszą możliwą ilość pomiarów i jednocześnie dowiedzieć się z nich, jak duża jest (co najmniej) ilość klucza kryptograficznego.

KM

Głównym rezultatem pracy jest podanie ograniczeń dolnych na wielkość klucza kryptograficznego, który można otrzymać przy pomocy publicznej komunikacji w jedną stronę (tzw. wielkości Devetaka-Wintera [DW05]) w terminach mierzalnych parametrów stanu. W tym celu stosujemy najpierw operacje symetryzacji stanu, tak aby uprościć jego postać. Pierwsze ograniczenie bazuje na pomiarze pojedynczej obserwabli, która jest odpowiednikiem świadka zasobu:

$$\hat{W}_{key} := (|11\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11|) \otimes U_{A'B'}, \tag{19}$$

gdzie U jest pewną transformacją unitarną, zależną od postaci stanu, którego bezpieczeństwo jest detektowane.
Jedno z wyprowadzonych ograniczeń w terminach $w := |\langle \hat{W}_{key} \rangle_\rho|$, tj. wartości średniej obserwabli $\hat{W}_{key}$, wynosi:

$$K_D \geqslant 1 - \sup_{0 \leqslant p_1+p_2 \leqslant 1,\, w \leqslant p_1 - p_2} [h(p_1+p_2) + H(p_1, p_2, \frac{1}{2}(1-p_1-p_2), \frac{1}{2}(1-p_1-p_2))], \tag{20}$$

gdzie h jest binarną entropią Shannona, zaś H to entropia Shannona. Wykazujemy też, że z powyższej nierówności można otrzymać mniej dokładne, ale za to prostsze ograniczenie postaci:

$$K_D \geqslant 1 - 2h(w) - h(\frac{1}{2}(1+w)), \tag{21}$$

które zależy od pojedynczego parametru stanu. Drugie ograniczenie bazuje na 2 parametrach: $w_z := |\langle \sigma_A^z \otimes \sigma_B^z \otimes \mathrm{I}_{A'B'} \rangle_\rho|$ oraz $w_x = |\langle \sigma_A^x \otimes \sigma_B^x \otimes U_{A'B'} \rangle_\rho|$, gdzie σ^x i σ^z to odpowiednie macierze Pauliego. W uproszczonej postaci wygląda ono następująco:

$$K_D \geqslant 1 - 2h(p_+) - (1-p_+)h(\xi_-^{min}) - p_+ h(\frac{w_x + w_z}{1+w_z}) \tag{22}$$

gdzie $p_\pm = 1/2(1 + \langle \sigma_A^z \otimes \sigma_B^z \otimes \mathrm{I}_{A'B'} \rangle_\rho)$, zaś $\xi_-^{min} = \max\{\frac{1}{2}, \frac{w_x+w_z}{1+w_z}\}$. W pracy podaliśmy również przykłady stanów bezpiecznych, w przypadku których ograniczenie górne jest ciasne i detektuje $K_D \approx 1$, w sytuacji gdy $E_D \to 0$ wraz z wymiarem układu $A'B'$ tegoż stanu.
Powyższe wyniki oprócz ustalenia analogicznego obiektu, tj. świadka bezpieczeństwa (19), wpisują się w szeroką wizję ekonomicznego detektowania zasobu (w podanym w pracy [H7] przykładzie wystarczył pomiar 6 ustawień, zamiast 81, których wymaga pełna tomografia stanu). Należy jednak pamiętać, że ceną za niewielką ilość pomiarów jest fakt, że ograniczenie dolne na klucz destylowalny skonstruowane z ich pomocą, nie jest optymalne.

2) **Ograniczenia powtarzaczy klucza kryptograficznego [H4]**
W pracy [H4] podjąłem się wraz ze współautorami zbadania następującego problemu:

- Czy klucz kryptograficzny w postaci dowolnego stanu mieszanego jest *przekazywalny*, tak jak ma to miejsce w przypadku stanów czystych, w którym kwantowy bezpieczny klucz i splątanie są sobie równoważne [Żuk+93, Ben+96b]?
- Czy klucz kryptograficzny zawarty w dowolnym stanie mieszanym jest *powtarzalny* za pomocą protokołu analogicznego do kwantowych powtarzaczy (ang. *repetares* [Dür+99]), tj. w przypadku dostępu do wielu kopii stanu kwantowego ?

Znalezienie odpowiedzi na te pytania jest niezwykle ważne z punktu widzenia przyszłości bezpiecznego Kwantowego Internetu. Gdyby były twierdzące, można by otrzymać nowe protokoły przekazywania bezpieczeństwa za pomocą tzw. *powtarzaczy klucza*.
Jak wykazaliśmy w [H4] przez podanie przykładów oraz ogólnych ogracznień dla pewnych klas stanów mieszanych, odpowiedź w obu przypadkach jest przecząca. Dowodzi to związku bezpieczeństwa kwantowego z nielokalnością Bella, gdzie nie ma możliwości przekazywania i powtarzania nielokalności [SPG06, Bar05].
Pokazaliśmy, że przekazywanie klucza kryptograficznego zawartego w stanie bezpiecznym $\gamma_{AA'C_1C_1'}$ i drugiej kopii tego samego stanu $\gamma_{C_2C_2'BB'}$ nie jest możliwe, poprzez sprowadzenie tego problemu do problemu odróżniania tychże stanów od stanów separowalnych za pomocą operacji LOKK. Ponieważ było wiadomo (jak zauważyłem uprzednio w ramach mojej tezy doktorskiej), że niektóre stany bezpieczne są słabo odróżnialne za pomocą operacji LOKK od pewnych stanów separowalnych $\hat{\gamma}_{ABA'B'}$, takiej postaci klucza (tj. reprezentowanej przez stan γ) nie można "przekazać",

KH

gdyż każdy taki protokół prowadziłby do odróżnienia γ od $\hat{\gamma}$, co, jak było wiadomo, nie jest możliwe. Mamy zatem wspomnianą analogię z nielokalnością Bella.
W scenariuszu kwantowych powtarzaczy klucza, stacje A, $C = C_1C_2$ i B współdzielą nie jedną, lecz dowolną ilość kopii stanu, zawierających klucz kryptograficzny. Celem jest wytworzenie w jak największej ilości klucza kryptograficznego współdzielonego pomiędzy A i B. Ilość tak "powtórzonego" klucza opisuje tzw. *klucz powtarzalny* postaci [H4]:

$$R^{A\leftrightarrow B\leftrightarrow C}(\rho_{AC_1}, \rho'_{C_2B}) = \inf_{\epsilon>0} \limsup_{n\to\infty} \sup_{\Lambda_n \in LOKK(A:C_1C_2:B),\gamma_m} \{\frac{m}{n} : Tr_C \Lambda_n((\rho_{AC_1} \otimes \rho'_{C_2B})^{\otimes n}) \approx_\epsilon \gamma_m\}, \quad (23)$$

gdzie $LOKK(A : C_1C_2 : B)$ to operacje LOKK między trzema układami: A, C_1C_2 oraz B. Główne rezultaty [H4] to wykazanie, przez przykład, że istnieją stany, które zawierają klucz kryptograficzny, a które jednocześnie mają klucz powtarzalny, zbiegający do zera z wymiarem stanu,

$$0 \approx R^{A\leftrightarrow B\leftrightarrow C}(\rho, \rho) < K_D(\rho) \approx 1. \quad (24)$$

Osiągnęliśmy ten cel podając ograniczenia górne na klucz powtarzalny. Pierwsze z nich, jest uogólnieniem przedstawionego podejścia do przekazywania klucza na przypadek wielu kopii:

$$\forall_{\rho,\rho'} \; R^{A\leftrightarrow B\leftrightarrow C}(\rho_{AC_1} \otimes \rho'_{C_2B}) \leqslant D^{\infty}_{C_1C_2\leftrightarrow AB}(\rho_{AC_1} \otimes \rho'_{C_2B}) \quad (25)$$

gdzie $D^{\infty}_{C_1C_2\leftrightarrow AB}(\rho_{AC_1} \otimes \rho'_{C_2B}) = \lim_{n\to\infty} \frac{1}{n} D_{C_1C_2\leftrightarrow AB}(\rho_{AC_1}^{\otimes n} \otimes \rho'_{C_2B}{}^{\otimes n})$, natomiast $D_{C_1C_2\leftrightarrow AB}(\rho \otimes \rho') = \inf_{\sigma\in SEP(C_1C_2:AB)} \sup_{M\in LOKK(C_1C_2:AB)} D(M(\rho\otimes\rho')||M(\sigma))$. Jakkolwiek ograniczenie wygląda na trudne do obliczenia, jak pokazujemy, można je oszacować od góry dla stanów o dodatniej częściowej transpozycji przez $2E_R(\rho^\Gamma)$ oraz $4I_{sq}(\rho^\Gamma)$, gdzie $\Gamma \equiv I \otimes T$ oznacza operację częściowej transpozycji. Czynniki 2 i 4 nie są optymalne, gdyż inną, prostą techniką wykazaliśmy lepsze ograniczenie dla stanów PPT oraz nieco słabsze, ale za to dla wszystkich stanów:

$$\forall_{\rho,\rho'\in PPT} \; R^{A\leftrightarrow B\leftrightarrow C}(\rho_{AC_1} \otimes \rho'_{C_2B}) \leqslant \min\{E^{\infty}_R(\rho^\Gamma), E^{\infty}_R(\rho'^\Gamma), I_{sq}(\rho^\Gamma), I_{sq}(\rho'^\Gamma)\}, \quad (26)$$

$$\forall_{\rho,\rho'} \; R^{A\to B\leftrightarrow C}(\rho_{AC_1} \otimes \rho'_{C_2B}) \leqslant \frac{1}{2}(E_D(\rho_{AC_1}) + E_C(\rho'_{C_2B})), \quad (27)$$

Powyżej $E^{\infty}_R(\rho) \equiv \limsup_{n\to\infty} E_R(\rho^{\otimes n})/n$, zaś układ strzałek $A \to B \leftrightarrow C$ opisuje fakt, że ograniczamy się w tym wypadku do protokołów, w których komunikacja przebiega od A do BC zaś między B i C jest w obu kierunkach.
Wykorzystując ograniczenie (27) podaliśmy konstrukcję stanu NPT, dokładniej stanu bezpiecznego, którego klucz powtarzalny zbiega do $\frac{1}{2}$, co wyklucza ten stan z użycia w scenariuszu wielu stacji pośrednich $C, D...$, gdyż przy wielu stacjach wykonujących protokół powtarzania [Dür+99] jego ilość znacznie maleje: mnożona przez czynnik $1/2^{k+1}$ w przypadku 2^{k+1} stacji pośrednich kwantowego powtarzacza klucza.
W pracy [H4] zadaliśmy również ogólne pytanie, dla jakich miar E zachodzi $E(\rho_{out}) \leqslant pE_D(\rho_{AC_1}) + (1-p)E(\rho'_{C_2B})$ gdzie stan ρ_{out} jest dowolnym stanem, który można osiągnąć za pomocą operacji $LOKK(A : C_1C_2 : B)$ ze stanów wejściowych ρ_{AC_1} i ρ_{C_2B}. Wykazaliśmy, że nierówność zachodzi nie dla wszystkich stanów wejściowych, w przypadku miar kosztu splątania oraz splątania formacji tj. gdy $E = E_C$ lub $E = E_F \equiv \inf_{\{p_i,\psi_i\}:\sum_i p_i|\psi_i\rangle\langle\psi_i| = \rho_{XY}} S(Tr_X|\psi_i\rangle\langle\psi_i|)$.
Jakkolwiek ograniczenie (25) nie jest optymalne, okazało się obiecującą techniką wykorzystaną w pracy [CF17], w której Matthias Christandl i Roberto Ferrara podali ograniczenie górne $2E_D^{\rightarrow}$ (tj. splątania destylowalnego za pomocą protokołów z komunikacją tylko w jedną stronę) na inną wersję klucza powtórzonego: $R^{C_1C_2\to A\leftrightarrow B}$. Dowód ten stanowi poważny krok na drodze do udowodnienia faktu, który wydaje się prawdziwy, że tylko w postaci czystego stanu kwantowego, klucz kryptograficzny jest "powtarzalny". Dowód tego faktu określiłby granice optymalności funkcjonowania przyszłego bezpiecznego Kwantowego Internetu.

3) **Nierogłaszalność nielokalności Bella [H6]**
Fakt, że nie można rozgłaszać kwantowego splątania za pomocą operacji LOKK tj. ze stanu ρ_{AB} stworzyć stanu $\rho_{ABA'B'}$ takiego, że $\rho_{AB} = \rho_{A'B'}$ jest prostą konsekwencją własności względnej entropii splątania, jak wykazujemy to w [H6]. W pracy tej wykazaliśmy, że analogicznie nie można rozgłaszać nielokalności Bella w przypadku nielokalnych rozkładów ze zbioru $NS(2,2,2,2)$

KM

za pomocą operacji do pewnego stopnia[6] analogicznych do operacji LOKK tj. przekształcających rozkłady lokalno-relistyczne w lokalno-realistyczne. Operacje te nazywane operacjami zachowującymi lokalność (OZL) które spełniają:

I) Λ jest poprawna, tj. przekształca niesygnalizujący rozkład warunkowy w niesygnalizujący rozkład warunkowy,

II) Λ przekształca w pełni niesygnalizujący rozkład warunkowy we pełni niesygnalizujący,

III) Λ przekształca lokalno-realistyczny rozkład warunkowy w lokalno-realistyczny.

gdzie rozkład warunkowy o $n \times m$ podukładach $I = \{A_1, ..., A_n, B_1, ...B_m\}$ nazywamy w pełni niesygnalizującym, jeśli dowolny podzbiór podukładów $J = \{A_{i_1}....A_{i_k}, B_{j_1}..., B_{j_l}\}$ nie sygnalizuje do pozostałych podukładów ze zbioru $I \setminus J$.
Główny rezultat [H6] to dowód faktu, że operacje spełniające powyższe aksjomaty nie mogą rozgłaszać nielokalności, tj.

$$\forall_{P_{AB} \in NS(2,2,2,2) \setminus L(2,2,2,2)} \{\Lambda(P_{AB}) = P_{ABA'B'}, Tr_{AB} P_{ABA'B'} = Tr_{A'B'} P_{ABA'B'} = P_{AB}\} \Rightarrow \Lambda \notin OZL \quad (28)$$

Aby udowodnić ten fakt, wprowadziliśmy nową miarę nazwaną anty-odporność $\bar{R}$:
$\bar{R}(P) = \max_{P' \in NS}\{q | qP + (1-q)P' \in L\}$, gdzie L to lokalno-realistyczne rozkłady warunkowe. Przedrostek "anty" oznacza, że przeciwnie do standardowych miar nielokalności, wielkość $\bar{R}$ *nie maleje* ze względu na operacje zachowujące lokalność. "Odporność" w nazwie odpowiada za fakt, że $\bar{R}$ mierzy w jakim stopniu rozkład warunkowy odporny jest na domieszanie innego, które skutkuje zmianą w rozkład lokalno-realistyczny. W pracy [H6] wykazujemy, że gdyby można było rozgłaszać rozkłady nielokalne, zmalałaby ich anty-odporność. Najpierw dowodzimy tę zależność dla rozkładów izotropowych - mieszanki rozkładu warunkowego B_{rst} oraz maksymalnie zmieszanego rozkładu warunkowego. Następnie zauważamy, że anty-odporność *nie zmienia się* ze względu na tzw. operacje które *uśredniają* (ang. "twirling"). Operacje uśredniające rzutują każdy rozkład warunkowy na jeden z odcinków $pB_{rst} + (1-p)B_{\bar{r}\bar{s}\bar{t}}$ $(0 \leqslant p \leqslant 1)$ w zależności od wartości bitów r, s (w przypadku $r = s = 0$ wprowadzone uprzednio w [MAG06, Sho09]). Jako że, jak pokazujemy, operacje te nie zmieniają wartości $\bar{R}$, sprowadziliśmy tym samym problem do już omówionego przypadku izotropowych rozkładów warunkowych. Argument powyższy stosuje się do rozkładów warunkowych, dla których odpowiednia nierówność $CHSH_{rst}$, jest większa od 3, wykazaliśmy jednak, że wszystkie rozkłady warunkowe, dla których nierówność $CHSH_{rst}$ wynosi 3, są lokalno-realistyczne.
Zwróćmy tutaj uwagę na fakt, że miara $\bar{R}$ może być interesująca niezależnie od poruszonego wyżej kontekstu. $1 - \bar{R}$ mierzy bowiem "odporność" rozkładu na szum, który w sposób naturalny pojawia się przy fizycznej realizacji rozkładów nielokalnych w laboratorium.

4) **Rozróżnialność rozkładów warunkowych za pomocą operacji zachowujących lokalność w sposób zupełny [H1]**
W analogii do problemu zbadanego w paradygmacie odległych laboratoriów, w pracy [H1] zadałem pytanie: jak dobrze można odróżnić ekstremalne niesygnalizujące rozkłady warunkowe (kwantowe oraz poza-kwantowe) wielościanu $NS(2,2,2,2)$ od siebie nawzajem? Aby odpowiedzieć na to pytanie przedstawiłem metodę analogiczną do znanej z teorii splątania - metodę Ghosh et al. [Gho+01].
W scenariuszu tym dwie osoby mają do dyspozycji jeden z rozkładów warunkowych (w ogólności zaszumiony) i nie wiedzą, który z nich współdzielą. Ich zadaniem jest zgadnąć z jak największym prawdopodobieństwem, który z rozkładów współdzielą, używając tylko (i) prostych pomiarów (odpowiadających ustaleniu wejść X, Y) oraz (ii) porównania otrzymanych wyników. Operację składającą się z tych dwóch, nazwałem operacją *porównującą* O_P. Aby móc zastosować analog metody Ghosh et al., wykazałem najpierw, że operacje O_P są operacjami w pełni zachowującymi lokalność (patrz równanie 28).
Główny rezultat stanowi nierówność wiążąca prawdopodobieństwo sukcesu rozróżnienia od siebie n izotropowych rozkładów warunkowych, tj. postaci $B_i^{\alpha_i} = \alpha_i B_{rst} + (1-\alpha_i)B_{\bar{r}\bar{s}\bar{t}}$, poprzez program

[6] Zauważmy, że operacje przekształcające rozkłady lokalno-realistyczne w rozkłady lokalno-realistyczne odpowiadają dokładnie w przypadku splątania operacjom przekształcającym zbiór stanów separowalnych w siebie. Te ostatnie jednak nie są LOKK, gdyż należy do nich opcracja zamiany podukładów, mamy tu więc tylko częściową analogię.

$p_s(5) \leq \frac{37}{40}$,	$p_s^{\alpha_q}(3) \leq 0.975593$
$p_s(6) \leq \frac{7}{8}$,	$p_s^{\alpha_q}(4) \leq 0.926778$
$p_s(7) \leq \frac{23}{28}$,	$p_s^{\alpha_q}(5) \leq 0.874817$
$p_s(8) \leq \frac{3}{4}$.	$p_s^{\alpha_q}(6) \leq 0.833334$
	$p_s^{\alpha_q}(7) \leq 0.785715$
	$p_s^{\alpha_q}(8) \leq 0.750001$

Rysunek 2: Po lewej stronie: ograniczenia na prawdopodobieństwo sukcesu odróżnienia od siebie za pomocą operacji porównujących elementów ansamblu $k \in \{5, ..., 8\}$ niesygnalizujących rozkładów warunkowych typu Popescu-Rohrlich ze zbioru $\{B^1_{rst} : r, s, t \in \{0, 1\}\}$. Ansambl jest postaci $\{\frac{1}{k}, B^1_{i_j}\}_{j=1}^k$, gdzie $i_j \in \{rst : r, s, t \in \{0, 1\}\}$. Po prawej stronie: ograniczenia na prawdopodobieństwo sukcesu odróżnienia od siebie za pomocą operacji porównujących elementów ansamblu $k \in \{3, ..., 8\}$ kwantowych rozkładów warunkowych łamiących maksymalnie odpowiednią nierówność $CHSH_{rst}$, tj. ze zbioru $\{B^{\alpha_q}_{rst} : r, s, t \in \{0, 1\}\}$, gdzie $\alpha_q = \frac{2+\sqrt{2}}{4}$. Ansambl jest postaci $\{\frac{1}{k}, B^{\alpha_q}_{i_j}\}_{j=1}^k$, gdzie $i_j \in \{rst : r, s, t \in \{0, 1\}\}$.

liniowy z kosztem nielokalności rozkładu warunkowego postaci $B_{in} := \sum_{i=1}^n \frac{1}{n} B_i^{\alpha_i} \otimes B_i^{\beta_i}$ ($B_i^{\beta_i}$ są zdefiniowane tak jak $B_i^{\alpha_i}$ tylko z innym parametrem):

$$\sum_i p(i,i)(\beta_i + \max_k \beta_k - 1) \leqslant \frac{C(B_{in}) + 3}{4} + \max_k \beta_k - 1. \tag{29}$$

W powyższej nierówności $p(i,i)$ to prawdopodobieństwo łączne zdarzenia, polegającego na tym, że współdzielony był rozkład $B_i^{\alpha_i}$ i odpowiedź osób zgadujących jest także i. $C(B_{in})$ zaś oznacza koszt nielokalności rozkładu B_{in}, gdzie w definicji kosztu (14) przez zbiór warunkowych rozkładów lokalno-realistycznych L przyjąłem mieszankę wypukłą produktów rozkładów, które są w pełni niesygnalizujące, zgodnie z definicją 1 podaną w [H6] i omówioną powyżej w punkcie 3.
Numeryczna analiza powyższego programu pozwoliła mi odnaleźć ograniczenia górne na rozróżnialność pewnej liczby układów (i) nielokalnych poza-kwantowych typu B^1_{rst} oraz pewnej liczby (ii) układów kwantowych typu $B^{\alpha_q}_{rst}$ dla $\alpha_q = \frac{2+\sqrt{2}}{4}$, czyli kwantowych rozkładów warunkowych łamiących maksymalnie odpowiednią nierówność $CHSH_{rst}$ (podsumowanie wyników przedstawiłem na Rys. 2).
Ponadto, w pracy [H1] wykazałem, że każda para ekstremalnych rozkładów niesygnalizujących (a więc reprezentujących wierzchołki wielościanu $NS(2,2,2,2)$), jest rozróżnialna konkluzywnie z niezerowym prawdopodobieństwem. Konkluzywność oznacza rozróżnienie, w którym, gdy (z pewnym prawdopodobieństwem) otrzymamy pewien wynik, jesteśmy pewni który z 2 rozkładów jest współdzielony. Wykazałem także, że układy lokalno-realistyczne są rozróżnialne między sobą konkluzywnie z prawdopodobieństwem 1, podobnie wszystkie rozkłady warunkowe ekstremalne w wielościanie $NS(2,2,2,2)$ są parami rozróżnialne z pewnością.
Powyższe badania mają znaczenie operacyjne, gdyż istotą przetwarzania informacji w sposób niezależny od urządzenia [Bru+14], jest opieranie się jedynie na statystykach ich wejść i wyjść. W takiej sytuacji naturalne staje się pytanie, w jakim stopniu można zidentyfikować dane urządzenie fizyczne, obserwując jedynie generowane przez niego statystyki.

5) **Ilościowanie kontekstualności [H5]**
W pracy [H5] zadaliśmy sobie pytanie, jak można mierzyć ilościowo kontekstualność. Zaproponowaliśmy dwie miary ekstensywne (tj. rosnące jako funkcja wymiaru rozkładu warunkowego). Pierwsza to *względna entropia kontekstualności.*[7] Miara ta jest zdefiniowana następująco:

$$X_{max}(P(a|c)) := \sup_{p(c)} \min_{N \in NC} \sum_c p(c) D(P(a|c)||N(a|c)), \tag{30}$$

gdzie $D(.||.)$ jest względną entropią [CT91], zaś $p(c)$ jest dowolnym rozkładem prawdopodobieństwa na zbiorze $\{1, ..., |\mathcal{C}|\}$, $|\mathcal{C}|$ jest liczbą kontekstów rozkładu warunkowego $P(a|c)$ zaś minimum

[7] Jak okazało się, w przypadku nielokalności analogiczna wielkość została zdefiniowana uprzednio [vGG05] pod nazwą "siła dowodu nielokalności".

przebiega po rozkładach warunkowych nickontekstualnych $N(a|c)$. Zauważmy tutaj pełną analogię do definicji miary splątania - względnej entropii splątania podanej w równaniu (4). Jak dowodzimy, miara ta jest równa innej mierze:

$$I_{max}(P(a|c)) := \sup_{p(c)} \min_{A(M_1,\ldots,M_{|\mathcal{M}|}|c)\equiv A_c \sim P(a|c)} I(\sum_c p(c)|c\rangle\langle c| \otimes A_c) \tag{31}$$

gdzie $A(M_1, ..., M_{|\mathcal{M}|}|c)$ jest rozkładem na wynikach wszystkich $|\mathcal{M}|$ obserwabli, zaś $A_c \sim P(a|c)$ oznacza, że rozkład marignalny wyników obserwabli z kontekstu c rozkładu A_c, jest taki sam jak rozkład $P(a|c)$[8]. I oznacza tu wspomnianą już wzajemną informację: $I(A : B) = H(A) + H(B) - H(AB)$, gdzie H to entropia Shannona.

Wielkość ta, choć wydaje się skomplikowana, może być rozumiana w terminach gry: Alicja chce przekazać numer kontekstu c Bogdanowi, zaś adwersarz, który przechwytuje c może wybrać rozkład A_c, jest jednak ograniczony do tych rozkładów, które na kontekstach są równe odpowiadającym im rozkładom $P(a|c)$. Jako że $X_{max} = I_{max}$, wykazaliśmy operacyjną interpretację względnej entropii kontekstualności. W pracy [H5] obliczyliśmy także wielkość tej miary dla wielu rodzin rozkładów warunkowych, takich jak *Peres-Mermin* [Per90, Mer90], *Rozkład Łańcuchowy* [Ara+12], *Gwiazda Mermina* [Mer93] i *KCBS* [Kly+08] oraz ich izotropowych wersji, tj. rozkładów warunkowych będących mieszanką wymienionych wyżej z rozkładem warunkowym, którego wszystkie konteksty mają rozkłady jednorodne. Miara ta pozwala porównywać kontekstualność różnych kontekstualnych rozkładów warunkowych.

Zbadaliśmy również addytywność miary X_{max} i wykazaliśmy, że jest addytywna na wierzchołkach wielościanu rozkładów nickontekstualnych o pewnych własnościach (np. takich jak rozkład Popescu-Rohrlich czy Peres-Mermin), tj. spełnia $X_{max}(P^{\otimes n}) = nX_{max}(P)$. Jest również addytywna w przypadku 2 kopii wspomnianych *izotropowych* rozkładów warunkowych. Wykazaliśmy również,

że w przypadku tych ostatnich rozkładów $X_{max} = X_u$, tj. mierze podobnej do X_{max}, dla której maximum po rozkładach na kontekstach w równaniu (30), jest zastąpione odwrotnością ich liczby. Podaliśmy jednak przykłady i scharakteryzowaliśmy ogólne rodziny rozkładów warunkowych, na których te dwie miary kontekstualności różnią się od siebie.

W pracy [H5] podaliśmy również definicję *kosztu nielokalności* oraz jego wartość dla rozkładu Peres-Mermin, który pod nazwą *frakcji kontekstualności* był, jak się okazało po opublikowaniu pracy, wprowadzony wcześniej w [AB11, Ams+12].

6) **Aksjomatyczne podejście do nielokalności Bella i kontekstualności [H2]**

Kwantowa kontekstualność była długo badana jako zjawisko, jednak nie była postrzegana jako zasób. Dopiero niedawno zostały podane przykłady zastosowania kwantowej kontekstualności, które wykazują jej użyteczność [How+14, SHP17]. Niemniej, jak każde zjawisko może ona być badana w ramach teorii zasobu: obiekty, które nie wykazują kontekstualności, tj. rozkłady niekontekstualne są darmowe [H2]. Taką właśnie perspektywę zaproponowaliśmy w pracy [H2]. Przedstawiliśmy w niej podejście do kontekstualności kwantowej i poza kwantowej oparte o kilka aksjomatów, analogicznych do tych znanych z teorii splątania [D1]. W oparciu o [Bar05] podaliśmy pewną klasę operacji O, która przekształca rozkład warunkowy w rozkład wyników. Zdefiniowaliśmy następnie metrykę (odległość dwóch rozkładów warunkowych od siebie), jako dystans wariacyjny rozkładów wyników, zmaksymalizowany po dozwolonej klasie operacji na rozkładach warunkowych: $||P - P'||_{box} = \sup_{M\in O} ||M(P) - M(P')||_{dist}$.

W pracy [H2], wykazaliśmy, że miara kontekstualności X_{max}, tj. *względna entropia splątania* (wprowadzona w [H5]), jest *asymptotycznie ciągła*, mianowicie jej wartości na bliskich sobie rozkładach warunkowych różnią się od siebie jedynie o czynnik zależny od logarytmu wymiaru[9]. Własność ta ma znaczenie dla eksperymentów detektujących kontekstualność, gdyż miara asymptotycznie ciągła nie jest wrażliwa na błędy przygotowania. Konkretnie, dla $||P - P'||_{box} \leqslant \epsilon$ zachodzi:

$$|X_{max}(P) - X_{max}(P')| \leqslant 30\epsilon \log d + 12\eta(1-\epsilon) + 18\eta(\epsilon) + 3\epsilon, \tag{32}$$

gdzie wymiar d wynosi $\min\{\Pi_{i=1}^{|\mathcal{M}|} a_i, |\mathcal{C}|\}$, zaś a_i to liczba możliwych wyników i-tej z $|\mathcal{M}|$

[8] W równaniu (31) użyliśmy notacji Diraca jedynie dla wygody, w istocie mowa tu o łącznym rozkładzie prawdopodobieństwa par (c, A_c).

[9] Z dokładnością do stałych oraz funkcji, która maleje do zera wraz ze zmniejszającą się odległością rozkładów

obserwabli, $|\mathcal{C}|$ to liczba kontekstów [10], natomiast $\eta(x) = -x\log_2(x)$. Powyższa nierówność pozostaje w analogii do asymptotycznej ciągłości względnej entropii splątania opisanej w równaniu (5).
Podaliśmy także ograniczenie górne miary X_{max} jako funkcję kosztu kontekstualności:

$$X_{max}(P) \leqslant \max\{X_{max}(P_v) : P_v\} \times C(P) \tag{33}$$

gdzie P_v jest wierzchołkiem wielościanu rozkładów warunkowych spełniających warunek konsystencji. Z uwagi na duży stopień ogólności dowodu tego faktu, własność tą posiadają wszystkie *wypukłe miary kontekstualności (i nielokalności).*
W pracy zastosowaliśmy także analog protokołu destylacji nielokalności przedstawiony w [FWW09], do rozkładów kontekstualnych. W tym celu wykazaliśmy, że protokół ten jest poprawny, tj. przekształca rozkład niekontekstualny w rozkład który też jest niekontekstualny. Następnie pokazaliśmy, że na pewnej klasie rozkładów prawdopodobieństwa, analogicznych do tych z [FWW09], rozkład wynikowy po zastosowaniu protokołu do 2 kopii rozkładu początkowego, w większym stopniu łamie pewną nierówność kontekstualną.

7) **Ograniczenia na kwantową nielokalność z wykorzystaniem częściowej transpozycji [H3]**
W pracy [H3] podajemy ograniczenie na miarę nielokalności *asymptotyczną względną entropię nielokalności.* Jest to miara względnej entropii kontekstualności rozkładu warunkowego, który pochodzi przez pomiar z wielu kopii tego samego dwuukładowego stanu kwantowego, podzielona przez liczbę kopii n (w granicy dużych n). Formalnie ma ona postać: [11]

$$R_N(\rho_{AB}) := \limsup_{n\to\infty} \frac{1}{n} \sup_{\Lambda\in LOKK} \sup_{M_{xy}} \mathcal{N}(\{Tr M_{xy}\Lambda(\rho_{AB}^{\otimes n})\}), \tag{34}$$

gdzie $\mathcal{N}(P(A,B|X,Y)) = \sup_{p(x,y)} \inf_{\Gamma_L\in L} \sum_{x,y} p(x,y) D(P(a,b|x,y)||P_L(a,b|x,y))$.
Jakkolwiek powyższa miara jest zdefiniowana w sposób trudny do obliczenia, jak wykazaliśmy, można podać proste ograniczenia górne na jej wielkość:

$$\forall_\rho \; R_N(\rho) \leqslant E_R(\rho) \tag{35}$$

$$\forall_{\rho\in PPT} \; R_N(\rho) \leqslant E_R(\rho^\Gamma) \tag{36}$$

Co zaskakujące, powyższe ograniczenie w przypadku stanów PPT jest tożsame z ograniczeniem na wielkość R (26), która opisuje powtarzalny klucz.
W pracy [H3] definiujemy także miarę (asymptotyczną) tzw. *ukrytej nielokalności*, tj. nielokalności generowanej ze stanu przez pomiar, otrzymywanej jedynie z pewnym prawdopodobieństwem p w wyniku postselekcji [Pop95]. Okazuje się, że miara zdefiniowana w sposób analogiczny do (34), jednak z uwzględnieniem multiplikatywnego czynnika p prowadzi do takiego samego ograniczenia jak w (36). Zatem, jak można było oczekiwać, nawet jeśli stan posiada dużą ukrytą nielokalność, można ją uzyskać z małym prawdopodobieństwem i stąd takie samo ograniczenie górne.
W przypadku pojedynczej kopii stanu podaliśmy także nierówność wiążącą stopień łamania nierówności Bella z rozróżnialnością od siebie dwóch stanów. Wykazaliśmy, że *różnica w łamaniu nierówności Bella w przypadku dwóch stanów jest proporcjonalna do stopnia ich odróżnienia za pomocą pewnej ograniczonej klasy operacji.* Istotnym przykładem zastosowania tej nierówności jest sprawdzenie jak łamią nierówności Bella stany bezpieczne, o których była mowa w sekcji 2.2. Dla stanów bezpiecznych słabo odróżnialnych od stanów separowalnych mamy istotne ograniczenie górne:

$$\mathbf{S}(\gamma_{AB}) \leqslant C(S) + Q(S) \times \inf_{\sigma\in SEP(A:B)} ||\gamma^\Gamma - \sigma^\Gamma||, \tag{37}$$

[10] Wymiar d w nierówności (32), w naszym odczuciu nie został w omawianej tu pracy opisany dostatecznie poprawnie jak i czytelnie, dlatego jego definicję, wraz z wyjaśnieniem innego przeoczenia, przedstawiliśmy w formie erraty (*Physical Review A* 99, 039901(E) (mar. 2019) [H2]). Oba niedopatrzenia nie zmieniają charakteru otrzymanych wyników, precyzują jedynie sposób otrzymania oraz formę otrzymanego wyniku - asymptotycznej ciągłości miary X_{max}.

[11] W pracy [H3] używamy w równaniu (34) notacji R, aby oznaczyć asymptotyczną względną entropię nielokalności. Zmieniamy tutaj tą notację na R_N, w celu odróżnienia od R oznaczającego pojęcie powtarzalnego klucza opisane w równaniu 23 zgodnie z notacją pracy [H4].

KH

gdzie $\mathbf{S}(\rho_{AB}) := \sum_{a,b,x,y} s^{a,b}_{x,y} Tr M^x_a \otimes M^y_b \rho_{AB}$ jest wartością nierówności Bella $S = \{s^{a,b}_{x,y}\}$ na stanie ρ_{AB}, zaś $Q(S)$ jest maksymalną wartością $S(\rho')$ dla wszystkich stanów kwantowych ρ', a $C(S)$ jest maksymalną wartością nierówności S osiąganą na rozkładach lokalno-realistycznych. Czynnik $||\gamma^\Gamma - \sigma^\Gamma||$, jak wykazałem uprzednio w doktoracie, bywa mały (rzędu $1/d$), dla niektórych stanów bezpiecznych. Zatem dla tych stanów możemy zaobserwować niewielki stopień łamania nierówności Bella o niewielkiej liczbie wejść i wyjść. Z uwagi na ten fakt, powyższa nierówność wyklucza wiele stanów bezpiecznych z użycia w *protokołach generowania klucza kryptograficznego niezależnego od urządzenia* [And98, BHK05, Ací+07], których faza akceptacji bazuje na obserwowaniu stopnia łamania takich nierówności Bella.
Powyższe wyniki wykazują, że badanie związków między bezpieczeństwem kwantowym a nielokalnością może prowadzić do ciekawych analogii, jak w przypadku ograniczenia (36). Stanowi ono również ważny temat, szczególnie w kontekście otrzymywania klucza kryptograficznego niezależnego od urządzenia.

5. Omówienie Pozostałych osiągnięć naukowo-badawczych

Ten podpunkt autoreferatu jest opisany następująco. Poniżej przedstawiam dane bibliometryczne. W sekcji 4 opisuję wyniki otrzymane przed doktoratem, a w kolejnej sekcji 5 wyniki otrzymane po uzyskaniu stopnia doktora. Sekcja 5.1 jest poświęcona opisowi publikacji spoza listy filadelfijskiej, opublikowane po doktoracie.

Dane bibliometryczne:

- Liczba publikacji z listy filadelfijskiej: **33** + 1 errata (**19** po doktoracie)
- Liczba wszystkich publikacji: **35** (w tym 1 publikacja pokonferencyjna oraz 1 pozycja książkowa) + 1 errata
- Sumaryczna liczba cytowań (według bazy Web of Science) **4301** (**4235** bez autocytowań), w tym:
  1) praca przeglądowa [D1] **3531** ($\geqslant$ **3510** bez autocytowań)
  2) pozostałe prace **770** ($\geqslant$ **704** bez autocytowań)
- H-index: **14**
- Sumaryczny współczynnik wpływu (ang. impact factor) **178,493**

4 Przed doktoratem

Moje zainteresowania badawcze w okresie przed doktoratem dotyczyły głównie możliwości przetwarzania stanów kwantowych w paradygmacie odległych laboratoriów. Paradygmat ten zakłada, że dwie (lub więcej) osób może wykonywać dowolne operacje kwantowe w swoich (odległych od siebie nawzajem) laboratoriach na zadanym stanie kwantowym, jak również komunikować się za pomocą klasycznych bitów, tj. wykonywać Lokalne Operacje kwantowe i Klasyczną Komunikację (LOKK). W scenariuszu tym badałem trzy zasoby: *klucz kryptograficzny bezpieczny względem kwantowego adwersarza* [D4, D3, D5, D6, D7, D8] jako miarę splątania, *kwantowe splątanie* [D9, D10], *kwantową czystość* (rozumianą jako ekwiwalent pracy termodynamicznej) [D11, D12, D13]. Badałem również ograniczenia operacji LOKK w kontekście *rozróżniania stanów kwantowych* [D2]. Ponadto w okresie przed doktoratem zostałem współautorem pracy przeglądowej opisującej zjawisko, jakim jest kwantowe splątanie [D1] (stan wiedzy na rok 2009), natomiast w pracy [D14] zajmowałem się bezpieczeństwem klucza kryptograficznego względem klasycznego adwersarza w analogii do kwantowego splątania.

W roku 2009 w pracy doktorskiej opisałem i pogłębiłem analizę wyników prac dotyczących klucza kryptograficznego bezpiecznego względem kwantowego adwersarza i kwantowego splątania [D4, D3, D5, D9]. W pracy tej zaobserwowałem również oraz zbadałem zjawisko nieodróżnialności niektórych stanów bezpiecznych od stanów separowalnych które powstają ze stanów bezpiecznych po zaatakowaniu ich części klucza.

Jednym z istotnych wyników badań nad kluczem kryptograficznym w przypadku bezpieczeństwa względem kwantowego adwersarza, było wykazanie, że jest on jedną z miar splątania K_D i może być badany w ramach teorii splątania [D4, D3]. Innym ważnym odkryciem dokonanym w tych pracach, było wykazanie,

że można otrzymać klucz kryptograficzny z bardzo zaszumionych stanów (o tzw. związanym splątaniu [HHH98], tj. splątanych, ale spełniających $E_D = 0$). Aby wykazać te fakty, scharakteryzowaliśmy stany kwantowe, które zawierają idealnie bezpieczny klucz, czyli tzw. *stany bezpieczne* [D4]. Wykazaliśmy, że operacje lokalne i publiczną komunikację można wykonać za pomocą operacji LOKK, gdy podsłuchująca osoba (zwykle zwana Ewą) otrzymuje puryfikację stanu kwantowego współdzielonego przez osoby uczciwe [D3] (szerzej przedstawione w mojej pracy doktorskiej). Ponadto w pracach [D4, D3] wykazaliśmy także, że ilość klucza kryptograficznego, którą można otrzymać ze stanu kwantowego jest ograniczona z góry przez względną entropię splątania [Ved+97] oraz wykazaliśmy kilka ważnych własności stanów bezpiecznych. W pracy [D5] podaliśmy przykłady stanów o niskim wymiarze i o związanym splątaniu, które mają niezerowy klucz kryptograficzny, który można otrzymać wykorzystując jedynie jednokierunkową komunikację klasyczną. W artykułach [D8, D7, D6] wypracowaliśmy analogiczny rezultat dla kanałów kwantowych, podając przykłady kanałów z niewielką kwantową pojemnością komunikacyjną [D8], a następnie z zerową kwantową pojemnością komunikacyjną [D7, D6] (tj. takie, przez które nie można wiernie przesyłać kubitów), które, jak dowiedliśmy, mają niezerową pojemność prywatną, tj. można przez nie przesyłać bezpiecznie klasyczne bity.

W pracy [D9] wykazaliśmy, że *koszt splątania* oraz *logarytmiczna ujemność* dla niektórych stanów zmieniają wartość z dużej wielkości do zera pod wpływem pomiaru lub śladu częściowego na *pojedynczym* kubicie stanu (inaczej - są blokowalne). Wykazaliśmy także, że względna entropia splątania nie ma tej własności (jest w tym sensie nieblokowalna).

W pracy [D10] wprowadziliśmy miarę wieloukładowego *zmniejszonego splątania* (ang. *squashed*) oraz udowodnili, że ogranicza z góry wieloukładowy klucz destylowalny.

W pracy [D11] wykazaliśmy ograniczenie na liczbę kubitów w stanie czystym (rozumianych jako ilość pracy termodynamicznej), które można otrzymać lokalnie z dwuukładowych stanów czystych za pomocą tzw. *ograniczonych zaszumionych operacji LOKK*. W pracy [D12] wykorzystaliśmy programowanie półdodatnio określone do zbadania ilości destylowalnej czystości z tzw. stanów Wernera [Wer89]. W pracy [D13] wykazaliśmy, że dwa zadania (i) otrzymywania lokalnie stanów czystych oraz (ii) otrzymywanie czystego splątania z dwuukładowych stanów są zadaniami komplementarnymi - otrzymywanie lokalnie dużej ilości stanów czystych uniemożliwia otrzymywanie dużej ilości stanów splątanych (i vice versa). Zdefiniowaliśmy także komutator dla operacji LOKK. Opisuje on sytuację, gdy dwie operacje komutują, gdy są wykonane na układzie globalnie, natomiast nie można wykonać ich jednocześnie na układzie za pomocą operacji LOKK.

5 Po doktoracie

W okresie po doktoracie, poza kontynuacją badań dotyczących klucza kryptograficznego [P1, P2] i kwantowego splątania [P3], moje zainteresowania badawcze skupiły się wokół własności zasobu nielokalności Bella [P4, P5, P6, P7] i szerzej, omówionej już kontekstualności oraz połączenia tych tematyk, jakim jest problem zwiększania bezpieczeństwa słabo prywatnej losowości [P8, P9, P10, P11].

W pracy [P3] wykazaliśmy że są stany, których podukładów nie można zamienić za pomocą operacji LOKK i zdefiniowaliśmy symetrię miar splątania i podali przykład miary, która jest asymetryczna. W pracy [P1] podaliśmy ze współautorami protokół otrzymywania klucza kryptograficznego ze stanu bezpiecznego, który daje w wyniku więcej klucza niż $\log d$, jeśli stan bezpieczny $\gamma_{ABA'B'}$ zawiera klucz w części $A'B'$ (zwanej tarczą). W pracy [P2] m.in. podaliśmy ograniczenie dolne na odległość stanów o dodatniej częściowej transpozycji (stanów PPT) od stanów bezpiecznych w przypadku $d = 2$, tj. bezpiecznych bitów. Podajemy również konstrukcje stanów PPT, które są niemal ortogonalne do stanów separowalnych. Dowodzimy także, że stany PPT w przypadku dostatecznie dużego wymiaru są odległe w normie śladowej od stanów separowalnych o $\approx 1/4$.

W pracy [P4] zbadaliśmy zjawisko wzrostu nielokalności Bella po wykonaniu operacji obwodowej (ang. wiring) na dwóch podukładach trzy-układowego rozkładu warunkowego. Podaliśmy ograniczenia dolne na koszt nielokalności oraz odporność nielokalności, wyrażone przez ilość nielokalności którą można uzyskać w ten sposób. Przedstawiliśmy również ograniczenie górne na nielokalność którą można uzyskać za pomocą operacji obwodowej, wyrażoną przez funkcję wagi komponentów rozkładu, które sygnalizują w przeciwną stronę do przebiegu operacji obwodowej. Zbadaliśmy numerycznie ilość nielokalności którą można uzyskać

AM

w badany tu sposób, dla kilku klas trójukładowych rozkładów warunkowych, w niektórych przypadkach osiągając optymalne rezultaty.

Prace [P5, P6] są poświęcone losowym kodom dostępu (LKD). Wykazaliśmy w nich m.in. równoważność LKD i funkcjonalności składającej się z rozkładu warunkowego Popescu-Rohrlich i możliwości przesłania 1 bitu komunikacji. Skonstruowaliśmy także sygnalizujący rozkład warunkowy, który nie jest w stanie symulować LKD. Następnie uogólniliśmy te rezultaty dla przypadku LKD pozwalającego na wybór jednego z n bitów oraz innych wariantów funkcjonalności LKD [P6].

W pracy [P7] uogólniamy grę CHSH do scenariusza gry posiadającej 3 wyniki i dowolną liczbę wejść, która współdzieli pewne cechy z grą CHSH. Gry te nazywamy grami XOR-3. Badamy zarówno nielokalność takich gier, jak i ich kontekstualność. Przedstawiamy także wyniki numeryczne ograniczeń górnych na kwantową wartość gier XOR-3 w przypadku niewielkiej (do 6) liczby wejść. Wykazaliśmy również, że gry typu XOR-d (dla $d \geqslant 2$) (również w przypadku więcej niż 2 graczy) nie mogą być pseudo-telepatyczne, tj. w przypadku kwantowym nie osiągają prawdopodobieństwa sukcesu 1.

W pracy [P12] wykazaliśmy do jakiego stopnia wartość nierówności Bella o jednym inpucie binarynym a drugim dowolnego rozmiaru n (nierówności $2 \times n$) w przypadku kwantowych rozkładów warunkowych różni się od wartości osiąganej maksymalnie przez rozkłady niesygnalizujące. Sformuowaliśmy w tym celu pojęcie nazwane frakcją dterminizmu (FD). Jak dowodzimy, w przypadku kwantowych rozkładów z wielościanu o rozważanej liczbie wejść, FD jest niezerowa. Kolejnym faktem, który wykorzystaliśmy a który jest interesujący sam w sobie, jest tzw. *odwrócona nierówność trójkąta* dla stanów kwantowych: *Jeśli k stanów jest odległych od innego o $2-\epsilon$, to ich kombinacja wypukła jest odległa od niego o conajmniej $2-2\sqrt{k\epsilon}$.*

W pracy [CR12] wykazano, że wykorzystując rozkłady łamiące prawie maksymalnie tzw. łańcuchową nierówność Bella (ang. "chain inequality"), można zwiększyć bezpieczeństwo losowości źródła Santha-Vasirani'ego z parametrem ϵ, jeśli ϵ jest odpowiednio małą dodatnią liczbą. W pracy [P8] wykazaliśmy dokładną wartość ϵ źródła słabej losowości Santha-Vasirani'ego, którego prywatność można wzmocnić za pomocą rozkładów typu łańcuchowego. Następnie w pracy [P9] podaliśmy protokół wykorzystujący niewielką liczbę urządzeń o niewielkiej liczbie podukładów, odporny na szum. W kolejnej pracy [P10] zredukowaliśmy liczbę urządzeń do 2. W ostatniej pracy z tego cyklu [P11] wykazaliśmy, że bezpieczeństwo losowości można wzmacniać, wykorzystując łańcuchową nierówność Bella, nawet wtedy, gdy adwersarz koreluje urządzenie z wartością bitów źródła Santha-Vasirani'ego za pomocą szerokiej klasy operacji.

5.1 Pozostałe publikacje

Praca [I1] określa, jak zmienia się dana nierówność Bella, jeśli wiemy, że ustawienia wejść X i Y są częściowo zależne od siebie. Publikacja książkowa [I2] to zestaw ćwiczeń do matematyki dyskretnej przeznaczona dla studentów pierwszego roku studiów informatyki. Obejmuje ona stadnardowy zestaw ćwiczeń dotyczących m.in. systemów obliczeniowych, kombinatoryki i rachunku prawdopodobieństwa.

Pozostałe prace opublikowane po doktoracie

[P1] Karol Horodecki, Piotr Ćwikliński, Adam Rutkowski i Michał Studziński. „On distilling secure key from reducible private states and (non)existence of entangled key-undistillable states". *New Journal of Physics* (grud. 2016), s. 083021. arXiv: 1612.08938.

[P2] Piotr Badziąg, Karol Horodecki, Michał Horodecki, Justin Jenkinson i Stanisław J. Szarek. „Bound entangled states with extremal properties". *Phys. Rev. A* 90.1 (lip. 2014), s. 012301. arXiv: 1309.7992.

[P3] Karol Horodecki, Michał Horodecki i Paweł Horodecki. „Are quantum correlations symmetric ?" *Quantum Inf. Comp.* (2010), s. 901–910. arXiv: quant-ph/0512224.

[P4] Jan Tuziemski i Karol Horodecki. „On the non-locality of tripartite non-signaling boxes emerging from wirings". *Quantum Inf. Comp.* (Sty. 2014), s. 1081–1108. arXiv: 1401.6973.

[P5] Andrzej Grudka, Karol Horodecki, Michał Horodecki, Waldemar Kłobus i Marcin Pawłowski. „When Are Popescu-Rohrlich Boxes and Random Access Codes Equivalent?" *Phys. Rev. Lett.* 113 (wrz. 2014), s. 100401. arXiv: 1307.7904.

KM

[P6] Anubhav Chaturvedi, Marcin Pawłowski i Karol Horodecki. „Random access codes and nonlocal resources". *Phys. Rev. A* 96, 022125 (sierp. 2017), s. 022125. arXiv: 1610.01268.

[P7] Piotr Gnaciński, Monika Rosicka, Ravishankar Ramanathan, Karol Horodecki, Michał Horodecki, Paweł Horodecki i Simone Severini. „Linear game non-contextuality and Bell inequalities - a graph-theoretic approach". *New Journal of Physics* (list. 2015), s. 045020. arXiv: 1511.05415.

[P8] Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Marcin Pawłowski i Ravishankar Ramanathan. „Free randomness amplification using bipartite chain correlations". *Phys. Rev. A* 90 (wrz. 2014), s. 032322. arXiv: 1303.5591.

[P9] Fernando G. S. L. Brandão, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Tomasz Szarek i Hanna Wojewódka. „Realistic noise-tolerant randomness amplification using finite number of devices". *Nature Communications* 7.1 (kw. 2016). arXiv: 1310.4544.

[P10] Ravishankar Ramanathan, Fernando G. S. L. Brandão, Karol Horodecki, Michał Horodecki, Paweł Horodecki i Hanna Wojewódka. „Randomness Amplification under Minimal Fundamental Assumptions on the Devices". *Phys. Rev. Lett.* (Kw. 2015), s. 230501. arXiv: 1504.06313.

[P11] Hanna Wojewódka, Fernando G. S. L. Brandão, Andrzej Grudka, Michał Horodecki, Karol Horodecki, Paweł Horodecki, Marcin Pawłowski, Ravishankar Ramanathan i Maciej Stankiewicz. „Amplifying the randomness of weak sources correlated with devices". *IEEE Trans. Inf. Theor.* (Sty. 2016), s. 7592–7611.

[P12] P. Joshi, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, Ben Li, S. J. Szarek i T. Szarek. „Bound on Bell inequalities by fraction of determinism and reverse triangle inequality". *Phys. Rev. A* 92 (wrz. 2015), s. 032329. DOI: 10.1103/PhysRevA.92.032329. arXiv: 1502.03088.

Prace opublikowane przed doktoratem

[D1] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki i Karol Horodecki. „Quantum entanglement". *Reviews of Modern Physics* 81 (kw. 2009), s. 865–942. arXiv: quant-ph/0702225.

[D2] Michał Horodecki, Aditi Sen De, Ujjwal Sen i Karol Horodecki. „Local indistinguishability: more nonlocality with less entanglement". *Phys. Rev. Lett.* 90 (sty. 2003), s. 047902. arXiv: quant-ph/0301106.

[D3] Karol Horodecki, Michał Horodecki, Paweł Horodecki i Jonathan Oppenheim. „General paradigm for distilling classical key from quantum states". *IEEE Trans. Inf. Theory*, quant-ph/0506189 (mar. 2005), s. 1898. arXiv: quant-ph/0506189.

[D4] Karol Horodecki, Michał Horodecki, Paweł Horodecki i Jonathan Oppenheim. „Secure Key from Bound Entanglement". *Phys. Rev. Lett.* 94 (kw. 2005), s. 160502. arXiv: quant-ph/0309110.

[D5] Karol Horodecki, Łukasz Pankowski, Michał Horodecki i Pawel Horodecki. „Low dimensional bound entanglement with one-way distillable cryptographic key". *IEEE Trans. Inf. Theory*, quant-ph/0506203 (czer. 2008), s. 2621–2625. arXiv: quant-ph/0506203.

[D6] Karol Horodecki, Michał Horodecki, Paweł Horodecki, Debbie Leung i Jonathan Oppenheim. „Unconditional Privacy over Channels which Cannot Convey Quantum Information". *Phys. Rev. Lett.* 100 (mar. 2008), s. 110502. arXiv: quant-ph/0702077.

[D7] Karol Horodecki, Michał Horodecki, Paweł Horodecki, Debbie Leung i Jonathan Oppenheim. „Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity". *IEEE Trans. Inf. Theory*, quant-ph/0608195 (czer. 2008), s. 2604–2620. arXiv: quant-ph/0608195.

[D8] Karol Horodecki, Debbie Leung, Hoi-Kwong Lo i Jonathan Oppenheim. „Quantum Key Distribution Based on Arbitrarily Weak Distillable Entangled States". *Phys. Rev. Lett.* 96 (lut. 2006), s. 070501. arXiv: quant-ph/0510067.

[D9] Karol Horodecki, Michał Horodecki, Paweł Horodecki i Jonathan Oppenheim. „Locking Entanglement with a Single Qubit". *Phys. Rev. Lett.* 94 (maj 2005), s. 200501. arXiv: quant-ph/0404096.

KH

[D10] Dong Yang, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim i Wei Song. „Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof". *IEEE Trans. Inf. Theory* (kw. 2009), s. 3375. arXiv: 0704.2236.

[D11] Michał Horodecki, Karol Horodecki, Paweł Horodecki, Ryszard Horodecki, Jonathan Oppenheim, Aditi Sende i Ujjwal Sen. „Local Information as a Resource in Distributed Quantum Systems". *Phys. Rev. Lett.* 90 (mar. 2003), s. 100402. arXiv: quant-ph/0207168.

[D12] Barbara Synak-Radtke, Karol Horodecki i Michał Horodecki. „Bounds on localizable information via semidefinite programming". *Journal of Mathematical Physics* 46 (sierp. 2005), s. 082107. arXiv: quant-ph/0405149.

[D13] Jonathan Oppenheim, Karol Horodecki, Michał Horodecki, Paweł Horodecki i Ryszard Horodecki. „Mutually exclusive aspects of information carried by physical systems: Complementarity between local and nonlocal information". *Phys. Rev. A* 68 (sierp. 2003), s. 022307. arXiv: quant-ph/0207025.

[D14] Karol Horodecki, Michał Horodecki, Paweł Horodecki i Jonathan Oppenheim. „Information Theories with Adversaries, Intrinsic Information, and Entanglement". *Foundations of Physics* 35, 12 (lip. 2005), s. 2027.

Publikacje spoza listy filadelfijskiej

[I1] Marcin Pawłowski, Karol Horodecki, Paweł Horodecki i Ryszard Horodecki "Local bounds for general Bell inequalities with the reduced entropy of the setting" W materiałach pokonferencyjnych konferencji NATO Advanced Research Workshop September 9-12, (2009), "Quantum Cryptography and Computing: Theory and Implementation" 224-230 (2010)

[I2] Hanna Furmańczyk, Karol Horodecki, Paweł Żyliński „Matematyka dyskretna dla studentów kierunku Informatyka" (w języku polskim - ćwiczenia z Matematyki Dyskretnej) ISBN 978-83-7326-708-4 Uniwersytet Gdański (2010)

Literatura

[AB11] Samson Abramsky i Adam Brandenburger. „The sheaf-theoretic structure of non-locality and contextuality". *New Journal of Physics* 13 (list. 2011), s. 113036. arXiv: 1102.0264.

[Ací+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio i Valerio Scarani. „Device-Independent Security of Quantum Cryptography against Collective Attacks". *Phys. Rev. Lett.* 98 (czer. 2007), s. 230501. arXiv: quant-ph/0702152.

[Ací+15] Antonio Acín, Tobias Fritz, Anthony Leverrier i Ana Belén Sainz. „A Combinatorial Approach to Nonlocality and Contextuality". *Comm. Math. Phys.* 334.2 (sty. 2015), s. 533–628. arXiv: 1212.4084.

[Ams+12] Elias Amselem, Lars Eirik Danielsen, Antonio J. López-Tarrida, José R. Portillo, Mohamed Bourennane i Adán Cabello. „Experimental Fully Contextual Correlations". *Phys. Rev. Lett.* 108 (maj 2012), s. 200405. arXiv: 1111.3743.

[And98] Dominic Mayers an Andrew Yao, red. *Quantum cryptography with imperfectapparatus* (Washington DC, USA). IEEE ComputerSociety, wrz. 1998, s. 503–509.

[Ara+12] Mateus Araújo, Marco Túlio Quintino, Daniel Cavalcanti, Marcelo França Santos, Adán Cabello i Marcelo Terra Cunha. „Tests of Bell inequality with arbitrarily low photodetection efficiency and homodyne measurements". *Physical Review A* 86.3 (wrz. 2012).

[Bar+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu i David Roberts. „Non-local correlations as an information theoretic resource". *Phys. Rev. A* 71 (2005), s. 022101. eprint: arXiv:quant-ph/0404097.

[Bar05] Jonathan Barrett. „Information processing in generalized probabilistic theories" (2005). arXiv: arXiv:quant-ph/0508211.

[BB84] Charles H. Bennett i Gilles Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing". W: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India, December 1984: IEEE Computer Society Press, New York, 1984, s. 175–179.

KM

[Bel64] J. S. Bell. *Physics (Long Island City, N.Y.)* 1 (1964), s. 195.

[Ben+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres i W. K. Wootters. „Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen Channels". *Phys. Rev. Lett.* 70 (1993), s. 1895–1899.

[Ben+96a] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu i Benjamin Schumacher. „Concentrating Partial Entanglement by Local Operations". *Phys. Rev. A* 53 (1996), s. 2046–2052. arXiv: quant-ph/9511030.

[Ben+96b] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin i William K. Wootters. „Purification of noisy entanglement and faithful teleportation via noisy channels". *Phys. Rev. Lett.* 76 (1996), s. 722–725. arXiv: quant-ph/9511027.

[Ben+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin i William K. Wootters. „Quantum nonlocality without entanglement". *Phys. Rev. A* 59 (1999), s. 1070–1091. arXiv: quant-ph/9804053.

[BHK05] Jonathan Barrett, Lucien Hardy i Adrian Kent. „No Signaling and Quantum Key Distribution". *Phys. Rev. Lett.* 95 (czer. 2005), s. 010503. arXiv: quant-ph/0405101.

[Bru+11] Nicolas Brunner, Daniel Cavalcanti, Alejo Salles i Paul Skrzypczyk. „Bound Nonlocality and Activation". *Phys. Rev. Lett.* 106 (sty. 2011), s. 020402. arXiv: 1009.4207.

[Bru+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani i Stephanie Wehner. „Bell nonlocality". *Reviews of Modern Physics* 86 (kw. 2014), s. 419–478. arXiv: 1303.2849 [quant-ph].

[BW92] C. H. Bennett i S. J. Wiesner. „Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". *Phys. Rev. Lett.* 69 (1992), s. 2881–2884.

[Cab08] Adán Cabello. „Experimentally Testable State-Independent Quantum Contextuality". *Phys. Rev. Lett.* 101 (list. 2008), s. 210401. arXiv: 0808.2456.

[CF17] Matthias Christandl i Roberto Ferrara. „Private States, Quantum Data Hiding, and the Swapping of Perfect Secrecy". *Phys. Rev. Lett.* 119 (grud. 2017), s. 220506. arXiv: 1609.04696.

[CFS16] Bob Coecke, Tobias Fritz i Robert W. Spekkens. „A mathematical theory of resources". *Information and Computation* (paź. 2016), s. 59–86. arXiv: 1409.5531.

[CG18] Eric Chitambar i Gilad Gour. „Quantum Resource Theories". *arXiv e-prints* (czer. 2018). arXiv: 1806.06107.

[Cla+69] J. F. Clauser, M. A. Horne, A. Shimony i R. A. Holt. „Proposed Experiment to Test Local Hidden-Variable Theories". *Phys. Rev. Lett.* 23 (1969), s. 880–884.

[CR12] Roger Colbeck i Renato Renner. „Free randomness can be amplified". *Nature Physics* 8 (czer. 2012), s. 450–454. arXiv: 1105.3195.

[CT91] T. M. Cover i Joy A. T. *Elements of information theory*. Wiley, 1991.

[CW04] M. Christandl i A. Winter. „"Squashed Entanglement": An additive entanglement measure". *J. Math. Phys.* 45 (2004), s. 829–840.

[DH99] M. J. Donald i M. Horodecki. „Continuity of relative entropy of entanglement". *Phys. Lett. A* 264 (1999), s. 257. arXiv: quant-ph/9910002.

[Die82] Dennis Dieks. „Communication by EPR devices". *Phys. Lett. A* 92 (1982), s. 271.

[Dür+99] W. Dür, H.-J. Briegel, J. I. Cirac i P. Zoller. „Quantum repeaters based on entanglement purification". *Phys. Rev. A* 59 (1999), s. 169–181. arXiv: quant-ph/9808065.

[DW05] I. Devetak i A. Winter. „Distillation of secret key and entanglement from quantum states". *Proc. R. Soc. Lond. A* 461 (2005), s. 207–235. arXiv: quant-ph/0306078.

[Egg+01] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner i M. M. Wolf. „Distillability via protocols respecting the positivity of partial transpose". *Phys. Rev. Lett.* 87 (2001), s. 257902. arXiv: quant-ph/0104095.

KH

[FWW09] Manuel Forster, Severin Winkler i Stefan Wolf. „Distilling Nonlocality". *Phys. Rev. Lett.* 102 (mar. 2009), s. 120401. arXiv: 1609.04696.

[Gho+01] S. Ghosh, G. Kar, A. Roy, A. Sen(De) i U. Sen. „Distinguishability of Bell States". *Phys. Rev. Lett.* 87 (2001), s. 277902. arXiv: quant-ph/0106148.

[HHH98] Michał Horodecki, Paweł Horodecki i Ryszard Horodecki. „Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?" *Phys. Rev. Lett.* 80 (1998), s. 5239–5242. arXiv: quant-ph/9801069.

[How+14] Mark Howard, Joel Wallman, Victor Veitch i Joseph Emerson. „Contextuality supplies the 'magic' for quantum computation". *Nature* 510 (czer. 2014), s. 351–355. arXiv: 1401.4174.

[Kly+08] Alexander A. Klyachko, M. Ali Can, Sinem Binicioğlu i Alexander S. Shumovsky. „Simple Test for Hidden Variables in Spin-1 Systems". *Phys. Rev. Lett.* 101 (lip. 2008), s. 020403. arXiv: 0706.0126.

[KS67] S. Kochen i E. P. Specker. „The problem of hidden variables in Quantum Mechanics". *J. Math. Mech.* 17 (1967), s. 59.

[MAG06] Ll. Masanes, A. Acín i N. Gisin. „General properties of nonsignaling theories". *Physical Review A* 73 (sty. 2006), s. 012112. arXiv: quant-ph/0508016.

[Mer90] N. D. Mermin. „Simple unified form for the major no-hidden-variables theorems". *Phys. Rev. Lett.* 65 (1990), s. 3373.

[Mer93] N. D. Mermin. „Hidden variables and the two theorems of John Bell". *Rev. Math. Phys.* 65 (1993), s. 803815.

[Per90] Asher Peres. „Incompatible results of quantum measurements". *Phys. Lett. A* 151 (1990), s. 107.

[Pop95] Sandu Popescu. „Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality". *Physical Review Letters* 74.14 (kw. 1995), s. 2619–2622.

[PR92] S. Popescu i D. Rohrlich. „Generic quantum nonlocality". *Phys. Lett. A* 166 (1992), s. 293.

[Sho09] Anthony J. Short. „No Deterministic Purification for Two Copies of a Noisy Entangled State". *Phys. Rev. Lett.* 102 (maj 2009), s. 180502. arXiv: 0809.2622.

[SHP17] Debashis Saha, Paweł Horodecki i Marcin Pawłowski. „State independent contextuality advances one-way communication" (sierp. 2017). arXiv: 1708.04751.

[SPG06] A. J. Short, S. Popescu i N. Gisin. „Entanglement swapping for generalized nonlocal correlations". *Phys. Rev. A* 73 (2006), s. 012101. arXiv: quant-ph/0508120.

[Tsi87] B. S. Tsirel'son. „Quantum analogues of the Bell inequalities. The case of two spatially separated domains". *J. Soviet. Math.* 36 (1987), s. 557–570.

[Tuc02] R. Tucci. „Entanglement of Distillation and Conditional Mutual Information". 2002.

[Ved+97] V. Vedral, M. B. Plenio, K. Jacobs i P. L. Knight. „Statistical Inference, Distinguishability of Quantum States, And Quantum Entanglement". *Phys. Rev. A* 56 (1997), s. 4452–4455. arXiv: quant-ph/9703025.

[vGG05] Wim van Dam, Peter Grunwald i Richard Gill. „The statistical strength of nonlocality proofs". *IEEE Trans. Inf. Theory* 51, quant-ph/0307125 (lip. 2005), s. 2812–2835. arXiv: quant-ph/0307125 [quant-ph].

[Wer89] R. F. Werner. „Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". *Phys. Rev. A* 40 (1989), s. 4277–4281.

[Wie83] S. Wiesner. „Conjugate coding". *Sigact news* 15:1 (1983), s. 78–88.

[WZ82] W. K. Wootters i W. H. Zurek. „A single quantum cannot be cloned". *Nature* 299 (1982), s. 802–803.

[Żuk+93] M. Żukowski, A. Zeilinger, M. A. Horne i A. Ekert. „"Event-ready-detectors" Bell experiment via entanglement swapping". *Phys. Rev. Lett.* 71 (1993), s. 4287–4290.

Gdańsk 17.04.2019
Karol Horodecki